3PAR
Serving Information

3PAR Recovery Manager 3.0.2 for Oracle on Solaris and Red Hat Linux User's Guide

3PAR Inc.
4209 Technology Drive
Fremont, CA 94538 U.S.A.

Part No. 320-200190 Rev A
November 2009

Revision Notice

This is the first release of this manual. A complete revision history is provided at the end of this manual.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, 3PAR Inc. assumes no liability resulting from errors or omissions in this document or from the use of the information contained herein.
3PAR reserves the right to make changes in the product design without reservation and without notification to its users.

Updates to the Documentation at 3PAR Central

Any updates to this document, or other 3PAR technical documents, can be found by logging into 3PAR Central's Document Control System from 3PAR's Support page, at: http://www.3PAR.com/support/index.html.

3PAR Technical Support and Services

Contact your local service provider for technical support and services.

Sales and Ordering Information

For sales and ordering information, contact
3PAR Inc.
4209 Technology Drive
Fremont, CA 94538 U.S.A.
Telephone: 510-413-5999
Fax: 510-413-5699
E-mail: salesinfo@3PAR.com

Reader Comments and Suggestions

E-mail your comments and suggestions about this document to: ReaderComments@3PAR.com

Copyright

Printed Material

Trademarks

Table of Contents

8 Using the Recovery Manager Rollback Utility

9 Using Remote Copy with Recovery Manager

1 Introduction

In this chapter

This user's guide provides the information needed to install, configure, and use the 3PAR Recovery Manager 3.0.2 for Oracle on Solaris and Red Hat Linux®. Recovery Manager offers a specific data protection solution that has been enhanced to provide rapid online recovery from space-efficient online point-in-time snapshots of an Oracle database. Further, Recovery Manager enables off-host backup of an Oracle database to tape, minimizing any impact to the production Oracle server.

1.1 Audience

This is an installation and configuration guide for system administrators and database administrators who are responsible for backing up databases and who understand Sun™ Solaris™ and/or Linux, and are familiar with the Oracle10*g*™ and Oracle11*g*™ Databases.

1.2 Related Documents

The following documents also provide information related to the InServ Storage Server:

For Information About...	Read the...
CLI commands and their usage	*3PAR InForm OS Command Line Interface Reference*
Identifying storage server components and detailed alert information	*3PAR InForm OS Messages and Operator's Guide*
Using the Command Line Interface (CLI) to configure and manage InServ Storage Servers	*3PAR InForm OS CLI Administrator's Manual*
Using the InForm Graphical User Interface (GUI) to configure and administer InServ Storage Servers	*3PAR InForm Management Console Online Help*
Using 3PAR Remote Copy	*3PAR Remote Copy User's Guide*

1.3 Organization

This guide is organized as follows:

- This chapter provides an overview of this guide, including intended audience, related documentation, typographical conventions, and advisories.
- Chapter 2, *Overview of Recovery Manager Operations*, provides an overview of 3PAR Recovery Manager and its utilities.
- Chapter 3, *Installing and Deinstalling Recovery Manager*, describes how to install, verify, and deinstall Recovery Manager for Oracle.
- Chapter 4, *Configuring Recovery Manager*, describes the steps for configuring Recovery Manager.
- Chapter 5, *Using Recovery Manager from the Menu-Driven Application*, provides an overview and instructions on using 3PAR Recovery Manager's menu-driven application.
- Chapter 6, *Using the Recovery Manager Command Line Interface*, introduces 3PAR Recovery Manager's command line interface and its commands.
- Chapter 7, *Using the Recovery Manager Graphical User Interface*, describes 3PAR Recovery Manager's Graphical User Interface.
- Chapter 8, *Using the Recovery Manager Rollback Utility*, describes how to use 3PAR Recovery Manager's rollback utility.
- Chapter 9, *Using Remote Copy with Recovery Manager*, provides an overview of how to use 3PAR Recovery Manager with 3PAR Remote Copy.
- This guide also contains an index and revision history for reference.

1.4 Typographical Conventions

The following typographical conventions are used in this guide:

Typeface	Meaning	Example
ABCDabcd	Used for dialog box elements such as titles and button labels.	Enter your system name in the **Value** box and click **OK**.
`ABCDabcd`	Used for file names, paths, and screen output, and for text you are to enter.	`Found < 12 > 73G disks.` Enter `cli` at the Windows command prompt.
<ABCDabcd>	Used for variables in file names, paths, and screen output, and variables in user input.	[root@(<systemID-nodeID>)root] `To continue Enter your system name ==> <systemname>`

1.5 Advisories

To avoid injury to people or damage to data and equipment, be sure to observe the cautions and warnings in this guide. ***Always be careful when handling any electrical equipment.***

NOTE: Notes are reminders, tips, or suggestions that supplement the procedures included in this guide.

CAUTION: Cautions alert you to actions that can cause damage to equipment, software, or data.

WARNING: Warnings alert you to actions that can cause injury to people or irreversible damage to data or the operating system.

2
Overview of Recovery Manager Operations

In this chapter

This chapter introduces virtual copy technology and provides instructions for using 3PAR Recovery Manager to back up and restore Oracle databases.

In this document, the following terminology is used:

- primary host - A host machine where the Oracle database installation occurs.
- backup host - A host machine where Recovery Manager for Oracle operations and backup media installation take place.

2.1 Virtual Copies

A virtual copy is a point-in-time image of a virtual volume created using the copy-on-write technique. It is composed of a pointer to the parent virtual volume and a record of all the changes made to the parent since the virtual copy was created. These changes can be rolled back to reproduce the parent's earlier state.

A virtual copy can be exported to or mounted on a server to allow regular operations such as backup or off-host processing.

Within 3PAR Recovery Manager, a virtual copy of a database is a point-in-time image of the database. It consists of virtual copies of the virtual volumes where the data files and/or archive logs reside. Recovery Manager can be used to create an online, offline, datafile, or archive log virtual copy of an Oracle database. An online or offline virtual copy is a point-in-time image of a database, which is taken while the database is OPEN (online) or CLOSED (offline), respectively. A datafile virtual copy is a point-in-time image of all database's datafiles, which is taken while the database is OPEN (online). An archive log virtual copy is a point-in-time image of database's archive log destination, which is taken while the database is online (OPEN).

Hereinafter, the term virtual copy is used to refer to a virtual copy of a database, rather than of a virtual volume.

2.2 About the Recovery Manager Repository

Information about virtual copies, database structures, and backup images (if backed up via Oracle RMAN and/or Veritas NetBackup) are stored in the 3PAR Recovery Manager repository when a virtual copy is created, or when a backup operation is performed. The information in the repository is used to manage virtual copies and to restore from a virtual copy backup image.

Some other Oracle-related files such as parameter files, password files, and control files are also saved in the Recovery Manager repository, along with the backup image information, for each virtual copy created.

The Recovery Manager repository is located in the following directory on the backup host:

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>
```

where:

- `<primary_host>` is the host name of the primary host.
- `<oracle_sid>` is the database ID.

The following example displays the location of the Recovery Manager repository on the backup host for Oracle database instance `test` that is running on primary host `Host1`.

```
/etc/3par/solutions/Host1.ora.test
```

If the database is a Real Application Cluster (RAC) database, there will be multiple repositories, one for each RAC instance.

2.3 Interacting with Oracle

3PAR Recovery Manager interacts with Oracle database through the SQL Plus utility to perform the following:

- Retrieve database structure information in order to create virtual copy for the database.
- Interact with the Oracle database (put tablespaces (or the whole database) in and out of backup mode, switch logfiles) as necessary to create a consistent virtual copy.

In order to create a consistent virtual copy of an Oracle database, the database structure must satisfy the following requirements:

- The database must be running in archive log mode and automatic archiving must be enabled in order to create an online virtual copy, datafile only virtual copy, or archive log only virtual copy.
- Datafiles and archive logs must reside on separate 3PAR virtual volumes.
- The online redo logs and control files should not reside on the virtual volumes used by the datafiles and archive logs to avoid being rolled back along with datafiles and archive logs virtual volumes. However, the online redo logs and control files can share the same 3PAR virtual volumes.
- If the database files reside on Veritas VxVM volumes, datafiles and archive logs must reside on separate VxVM disk groups. The online redo logs and control files should reside on separate VxVM volumes used by the datafiles and archive logs.
- If the Oracle database is an ASM managed database, the datafiles and archive logs must reside on separate ASM disk groups. The online redo logs and control files should not reside on the same ASM disk groups used by the datafiles and archive logs to avoid being restored when using the Recovery Manager Rollback feature.
- ASM disk groups should not be shared between different databases.
- If the database is an RAC database, all RAC instances must share the same archive log destinations (same cluster file systems or same ASM disk groups).

To ensure that the database is running in automatic archive log mode, use SQL Plus to ensure that the `Database log mode` is `Archive Mode` and that `Automatic archival` is `Enabled`, as in the following example:

```
$ sqlplus "/as sysdba"

SQL*Plus: Release 9.2.0.1.0 - Production on Wed Nov 14 13:59:13 2007
Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.1.0 - 64bit Production
With the Partitioning, Real Application Clusters, OLAP and Oracle Data
Mining options
JServer Release 9.2.0.1.0 - Production

SQL> archive log list
Database log mode                   Archive Mode
Automatic archival                   Enabled
Archive destination                  /rac9i_db/rac9i_arch2
Oldest online log sequence      764
Next log sequence to archive   764
Current log sequence               765
```

2.4 Interacting with Veritas Volume Manager

Due to restrictions on VxVM, 3PAR Recovery Manager requires a minimum of two disk groups per database.

CAUTION: The archive log destination must reside on a different Veritas disk group than any of the disk groups that contain data files for backup operations. It is also recommended that all database data files be in one VxVM disk group.

Because of the Veritas VxVM disk group limitation of allowing only one imported VxDG per disk group, Recovery Manager allows only one virtual copy per database to be mounted at a time. You must unmount the virtual copy for a database after it has been backed up in order to mount another virtual copy.

2.5 Interacting with Veritas NetBackup and Oracle RMAN

3PAR Recovery Manager integrates 3PAR Virtual Copy with Veritas NetBackup (NBU) and Oracle RMAN to dramatically reduce the performance impact on the database host, as well as to minimize database down time during backup. Instead of a traditional backup where the database is backed up directly on the production server, Recovery Manager creates a virtual copy (snapshot) of the database, imports it to a secondary host (backup host), and then performs the backup of the virtual copy on the backup host.

Recovery Manager provides two ways to perform backup and restoration: NBU (user-managed) and Oracle RMAN.

NOTE: For an ASM managed database, Oracle RMAN backup is the only supported backup method.

For NBU (user-managed) backup and restoration, Recovery Manager interacts directly with NBU to trigger the backup/restore process. Recovery Manager requires that the NBU client must be installed on the primary (database) server and the backup host.

For Oracle RMAN backup, Recovery Manager supports backup to tape and backup to disk. If Recovery Manager is configured to perform backup to disk, Recovery Manager interacts with Oracle RMAN to trigger the backup process. If Recovery Manager is configured to perform backup to tape, Recovery Manager interacts with Oracle RMAN, which in turn interacts with NBU to trigger the backup/restore process. Recovery Manager requires that Oracle database software (Oracle RMAN) and Veritas NetBackup Client must be installed on the primary host and the backup host. Additionally, Veritas NetBackup for Oracle (Oracle Agent) must be installed on the primary host, backup host, and NetBackup master server, if you select to backup to tape.

Recovery Manager requires that at least one NBU policy must be created per database. Optionally, a separate NBU policy can be created for archive log backup (backup archive log only). The NBU policies must be created as "standard" type or "Oracle" type for NBU (user-managed) backup/restore or Oracle RMAN backup/restore, respectively (see *4.7 Setting Up NetBackup Policies for NBU (User-Managed) Backup* on page 4.19 or *4.8 Setting Up NetBackup Policies for Oracle RMAN Backup* on page 4.22 for detailed information).

2.6 Recovery Manager Utilities

Read this section for general information regarding 3PAR Recovery Manager utilities available through the Recovery Manager command line interface, menu driven application, and graphical user interface.

2.6.1 The Database Configuration Utility

3PAR Recovery Manager's database configuration utility (`vcdba_config`) creates a Recovery Manager configuration file for each database instance. All operations that are available from Recovery Manager require this configuration file. After the Recovery Manager configuration file is created for a database instance, it is stored at:

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config
```

An equivalent environment file is also created for each configuration file. It contains all configuration options that are specified in the configuration file. Recovery Manager uses the environment file for its operations. The environment file is also stored at the same location as the configuration file.

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config_exp.sh
```

If a configuration file of a database instance exists, it is overwritten. The permission of the configuration file is set to the user that created the file.

2.6.2 The Virtual Copy Creation Utility

3PAR Recovery Manager's create utility creates an online, offline, datafile, or archive log virtual copy of an Oracle database (`vcdba_create` command).

- online or offline virtual copy - A point-in-time snapshot image of a database while it is OPEN (online) or CLOSED (offline).
- archive log virtual copy - A snapshot image of the archive log destination of a database while it is online (OPEN).
- datafile virtual copy - A point-in-time snapshot image of the datafiles of a database while the it is online (OPEN). A datafile virtual copy alone cannot be used for recovery without the archive logs generated up to the point when the virtual copy is taken. It is assumed that the user is responsible for making sure all required archive logs exist.

Once created, the virtual copy can be mounted on the backup host for off-host processing purposes such as backup and database cloning.

A database virtual copy consists of multiple virtual copies of underlying 3PAR virtual volumes used by Oracle datafiles, archive log destination, or both, depending on which option is specified (online, offline, datafile, or archonly). An archive log virtual copy can be used in conjunction with online or offline virtual copy to simulate an incremental backup.

If Recovery Manager is configured to use Oracle RMAN for backup, an RMAN Recovery Catalog must have been created and configured prior to running the create utility. The Recovery Manager create utility performs Recovery Catalog synchronization during the virtual copy creation process.

When creating an online virtual copy, the create utility performs the following actions:

- Discovers devices (3PAR virtual volumes) used by the datafiles and archive log destination.
- Puts all tablespaces in backup mode.
- Creates a virtual copy for the datafile virtual volumes.
- Takes all tablespaces out of backup mode.
- Switches online redo logs and archives them to archive log destination.
- Resynchronizes the Recovery Catalog to update with newly generated archive logs if the virtual copy is to be backed up using Oracle RMAN.
- Creates a virtual copy for the archive log destination virtual volumes.

An offline virtual copy is created while the database is CLOSED. The create utility will perform the following actions:

- Starts up the database in MOUNTED mode to retrieve list of datafiles and shuts down the database.
- Discovers devices (3PAR virtual volumes) used by the datafiles.
- Creates a virtual copy for the datafile virtual volumes.

An archive log virtual copy is created while the database is OPEN and performs the following actions:

- Discovers devices (3PAR virtual volumes) used by the archive log destination.
- Switches logs and archives online redo logs to archive log destination.

- Resynchronizes the Recovery Catalog to update with newly generated archive logs if the virtual copy is to be backed up using Oracle RMAN.
- Creates a virtual copy for the archive log destination virtual volumes.

NOTE: If the virtual copy is to be backed up using Oracle RMAN, a Recovery Catalog must have been created and configured prior to running this utility. For an RAC database, archive log destinations of all RAC instances must be on shared storage (same cluster file systems or same ASM disk groups).

2.6.3 The Virtual Copy Display Utility

3PAR Recovery Manager's display utility (`vcdba_display`) displays database virtual copies along with other information including creation time, type, status, and backup status.

A virtual copy's type can be either Online, Offline, Datafile, or Archlog.

- An Online virtual copy indicates that the virtual copy for the database was created while it was OPEN (online).
- An Offline virtual copy indicates that the virtual copy for the database was created while it was CLOSED (offline).
- A Datafile virtual copy indicates that the virtual copy for the database was created while it was OPEN (online) and contains only datafiles (no archive log destination).
- An Archlog virtual copy indicates that the virtual copy was created for archive log destination only.

A virtual copy's status can be either `Available`, `Removed`, `Mounted`, `Mounted(P)`, or `Database`.

- `Available` status indicates that the virtual copy exists and is not currently mounted or cloned.
- `Removed` status indicates that the virtual copy is removed.
- `Mounted` status indicates that the virtual copy is currently mounted.
- `Mounted(P)` status indicates that the virtual copy is partially mounted.
- `Database` status indicates that a database has been cloned using the virtual copy.

A virtual copy's backup status can be either Y or N, where Y indicates that the virtual copy has been backed up and N indicates that the virtual copy has not been backed up.

2.6.4 The Virtual Copy Mount Utility

3PAR Recovery Manager’s mount utility mounts an existing database virtual copy that was created using the create utility on the backup host using the `vcdba_mount` command. The mounted virtual copy can be used for off-host processing purposes such as backup or database cloning.

The following restrictions apply when mounting a database virtual copy:

- The virtual copy must have an `Available` or `Mounted(P)` status in order to be mounted. The virtual copy's status can be retrieved using the Recovery Manager display utility.
- The same virtual copy cannot be mounted concurrently at different mount points.
- If the database files reside on Veritas VxVM Volumes, only one virtual copy per database can be mounted at any time on the backup host. This is due to the VxVM disk groups from different virtual copies of the same database having the same names and so cannot be imported at the same time.
- If the database files reside on ASM disk groups, it is dependent on which ASM database version is installed on the backup host, different restrictions apply as follows:
    - If the ASM version on the backup host is 10.2.0.5 or 11.1.0.7, one virtual copy per database can be mounted at any time on the backup host. However, virtual copies from different databases can be mounted concurrently.
    - If the ASM version on the backup host is lower than the releases mentioned in the previous bullet, only one virtual copy can be mounted at any time on the backup host. This restriction prevents an Oracle ASM instance on the backup host from hanging due to some ASM's idle processes still holding a virtual copy's devices, even though the corresponding ASM disk groups are dropped.
- If the database files reside on OCFS2 file systems, only one virtual copy per database can be mounted at any time on the backup host.

Mounting a database virtual copy involves the following actions:

- A read-write virtual copy of the original (read-only) virtual copy is created.
- The read-write virtual copy is imported to the backup host.
- Snapshots of Veritas VxVM disk groups are imported and all corresponding snapshot VxVM volumes are started if the database files reside on VxVM volumes.
- All snapshot file systems are mounted if the database files reside on file systems.

- For virtual copies from an ASM-managed database, based on the different ASM database releases on the backup host, the operation is different.
    - For ASM versions 10.2.0.5 or 11.0.1.7, if an ASM instance exists and is up on the backup host, then all diskgroups from the virtual copy are mounted in this ASM instance. Otherwise, an ASM instance is started up on the backup host, and all ASM disk groups in the virtual copy are mounted.
    - For ASM versions lower than the releases mentioned in the previous bullet, if an ASM instance is up on the backup host, the mount utility checks if there is any mounted diskgroup. If none, the ASM instance is shut down, otherwise, the mount utility gives an error and exits. After that, a new ASM instance is started up and all diskgroups contained in the current virtual copy are mounted.

2.6.5 The Virtual Copy Unmount Utility

3PAR Recovery Manager's virtual copy unmount utility (`vcdba_umount`) unmounts the file system where a virtual copy is currently mounted. The read/write virtual copy is removed, as well as any components that were created during the mount virtual copy stage.

The virtual copy must have `Mounted` or `Mounted(P)` status in order to be unmounted. The status of a virtual copy can be obtained using a display utility such as the `vcdba_display` command.

Unmounting a database virtual copy involves the following actions:

- For an ASM-managed database, if the ASM database on the backup host has a version at or above 10.2.0.5 or 11.1.0.7, unmounting the virtual copy drops the ASM diskgroups that are contained in the virtual copy and cleans up the ASM disks.
- If the ASM database on the backup host has versions lower than those listed in the previous bullet, unmounting shuts down the ASM instance and cleans up ASM disks.
- Unmounts all snapshot file systems if the database files reside on file systems.
- Destroys all snapshot VxVM disk groups and their VxVM volumes if the database files reside on VxVM volumes.
- Deports the read-write virtual copy from the backup host.
- Removes the read-write virtual copy.

2.6.6 The Virtual Copy Export Utility

3PAR Recovery Manager's virtual copy export utility exports an existing virtual copy to an alternate backup host. The exported virtual copy (`vcdba_export` command) can then be mounted, backed up or cloned at the alternate backup host.

The virtual copy must have `Available` status in order to be exported. An alternate backup host must have the same operating system, file system, volume manager, and Recovery Manager version as the current backup host. Status of a virtual copy can be obtained using a display utility such as the `vcdba_display` command.

The following restrictions apply to exporting virtual copies:

- If Veritas Volume Manager is used, the alternate backup host must have the same version of Veritas Volume Manager that is currently installed.
- The alternate backup host must be connected to the same InServ Storage Server as the current backup host.
- An identical Oracle Database Administrator user ID and group ID on the backup host must exist on the alternate backup host.
- If the backup host uses SSH as the connection method from the backup host to the primary host, then a secure shell connection must be set up between the backup host and the alternate backup host prior to executing this utility. This is the only connection method supported in Red Hat Linux.
- (Solaris only) If the backup host uses RSH as the connection method from the backup host to the primary host, then an RSH connection must be set up between the backup host and the alternate backup host prior to using this utility.
- Once exported, the virtual copy on the alternate backup host can be mounted, umounted, backed up, and restored.
- Once the exported virtual copy is no longer needed, its repository can be removed from the alternate backup host.

2.6.7 The Database Cloning Utility

3PAR Recovery Manager's database cloning utility (`vcdba_createdb` command) creates a single-instance database, or starts up a cloned database in MOUNTED mode for backup (RMAN) purposes. A single-instance database can be used for any off-host processing purpose. A cloned database that is started in MOUNTED mode, can be used for RMAN backup.

The virtual copy used for cloning a database must be either an online or offline virtual copy (created using the `vcdba_create` or `vcdba_sync` command). The virtual copy must have been mounted using the `vcdba_mount` command prior to running this command.

A clone database can be created using an ascii or binary controlfile which was saved in the Recovery Manager repository at the time the virtual copy was created. Using an ascii controlfile is more flexible as it allows you to change database instance name as well as the structure of the database.

When using an ascii controlfile, the structure of the clone database is not required to be exactly the same as the structure of the primary (original) database. Therefore the virtual copy can be mounted at any mount point. However, since the virtual copy does not contains online redo-logs and control files, their locations can be specified using the `-d` option (can be one or more directories or ASM diskgroups, depending on the desired multiplexing). The number of multiplex redo log locations must be equal to, or less than, the primary database when creating the clone database. Otherwise, the extra redo log multiplex location will be ignored. If the locations of the redologs and controlfiles are not specified, they will be created at the repository location for the virtual copy (`/etc/3par/solutions/<host>.ora.<sid>/<vc_name>`).

When using a binary controlfile the structure of the clone database must be exactly the same as the structure of the primary database. Therefore, the virtual copy must be mounted at '/' if the datafiles and archive logs are on file systems. Also, since the virtual copy does not contain redologs and archivelogs, the same directory structure or same ASM diskgroups for the redologs and controlfiles must be pre-created on the backup host.

When creating a clone database for backup (RMAN) purposes, the database is started in MOUNTED mode using the binary controlfile from the repository without recovering the database. This can be achieved by using the `-o for_backup` or `-o binary, norecovery` option.

A clone database can be created with or without automatic recovery (applying archivelogs from the virtual copy) using the `–o recovery` or `-o norecovery` option. If recovery is chosen the clone database is open with a reset log, otherwise, the clone database is in a mounted status.

2.6.8 The Cloned Database Removal Utility

3PAR Recovery Manager’s cloned database removal utility (`vcdba_removedb` command) removes a cloned database, which was created using the `vcdba_createdb` command.

The cloned database is shutdown with the `shutdown immediate` option. All files (Oracle parameter file, control files, and redo logs), which were previously created by the `vcdba_createdb` command, are removed. The virtual copy remains mounted.

2.6.9 The Virtual Copy Removal Utility

3PAR Recovery Manager’s virtual copy removal utility removes an existing virtual copy from the InServ storage system. The virtual copy must have `Available` status in order to be removed using the `vcdba_remove` command. The status of a virtual copy is obtained by using the display utility `vcdba_display`.

This utility only removes the read-only virtual copy from the system to free up the snapshot space. It does not actually remove the repository information if the virtual copy has been backed up to the media. This enables Recovery Manager to restore a virtual copy, which has been previously backed-up to the media on the original volume, as long as the virtual copy repository exists.

2.7 The Virtual Copy Repository

3PAR Recovery Manager records important information for each virtual copy taken by the Recovery Manager utilities. The information is used by Recovery Manager for database restoration. The information is stored in the repository at:

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/<timestamp>
```

2.7.1 The Virtual Copy Repository Removal Utility

3PAR Recovery Manager’s virtual copy repository removal utility removes a virtual copy’s repository that was created using the create utility (*2.6.2 The Virtual Copy Creation Utility* on page 2.7). The virtual copy that has been removed must have Removed status in order for Recovery Manager to remove the repository. The status of a virtual copy can be obtained using the display utility (*2.6.3 The Virtual Copy Display Utility* on page 2.9).

If a virtual copy has been backed up, the remove repository utility command fails unless the `-f` option is used.

2.8 Virtual Copy Policy

3PAR Recovery Manager provides the capability to limit the maximum number of virtual copies allowed per database instance at any time.

For example, a policy can be set to only allow twelve virtual copies at any time for a database. Recovery Manager always maintains the twelve latest virtual copies by removing the oldest virtual copy before creating a new copy. The default, and maximum allowed, number is 500, meaning that up to 500 read-only virtual copies can be created if you have sufficient snapshot space.

2.9 Database Rollback from a Virtual Copy

When a database is corrupted, you can restore the database to the most recent database images from the most recently created virtual copy by using the rollback utility.

2.9.1 The Database Rollback Utility

3PAR Recovery Manager's database rollback utility (`vcdba_rollback`) promotes a virtual copy's volumes back to its base virtual volumes. In other words, the base virtual volumes used by the database are rolled back to the virtual copy volumes. Once the rollback process completes successfully, the base virtual volumes are exactly the same as the virtual copy volumes. If the base volume size has been changed since the virtual copy was taken, the rollback process will not affect the new size.

- When rolling back from an online virtual copy, both datafile and archive log virtual volumes are rolled back by default. Use the `-o` option to rollback only datafile virtual volumes or only archive log virtual volumes.
- When rolling back from an offline virtual copy, only datafile virtual volumes are rolled back.
- When rolling back from an archive log virtual copy, only archive log virtual volumes are rolled back.

The following restrictions apply when rolling back a virtual copy:

- The online redo logs and control file should not reside on the same virtual volumes used by the datafiles and archive logs. Otherwise, they will be rolled back along with the datafile and archive log virtual volumes.

- The database instance must be CLOSED for this operation. If the database is an RAC database, all RAC instances must be CLOSED.
- The base (datafile and/or archive log) virtual volumes must be temporarily removed from the primary (database) server.
- The specified virtual copy must have an `Available` status (not mounted).

Recovery Manager saves an ASCII control file and a binary control file for each created virtual copy in its repository. After a rollback, you may need to restore the control file in order to perform database recovery.

2.10 Recovery Manager and Third-Party Backup Tools

3PAR Recovery Manager integrates 3PAR Virtual Copy with Veritas NetBackup (NBU) and/or Oracle RMAN to perform off-host backup. Off-host backups can dramatically reduce performance impact on the primary host and minimize database down time or database in backup mode during backup.

Recovery Manager creates a virtual copy (snapshot) of the database, mounts it to the backup host, then performs backup of the virtual copy.

Recovery Manager supports online(hot), offline(cold), datafile, or archive log backups.

- Online backup - A database backup while it is OPEN.
- Offline backup - A database backup while it is CLOSED.
- Datafile backup - A backup of datafiles only.
- Archive log backup - A backup of archive logs only.

Recovery Manager can be configured to perform either NBU (user-managed) backup or Oracle RMAN backup (See *4.9 Recovery Manager Configuration Files* on page 4.27 for details).

2.10.1 The Database Backup Utility

3PAR Recovery Manager’s database backup utility supports full and/or incremental backup of an Oracle database or archive log destination. Full backup of an Oracle database or archive log destination are always supported regardless of backup method (NBU backup or Oracle RMAN backup). However, incremental (differential or cumulative) backup of a whole Oracle database is only available using Oracle RMAN backup. Incremental (differential or cumulative) backup of archive log destination is only available for the NBU (user-managed) backup method.

The following restrictions apply when backing up a database using the Recovery Manager database backup utility.

- For NBU (user-managed) backup:
  - The NBU client must be installed on the backup host, as well as on the primary host.
  - At least one NBU policy of standard type must be created and configured for database backup. Optionally, a separate NBU policy of standard type can be created and configured for archive log destination backup.
- For Oracle RMAN backup:
  - If RMAN sbt_tape backup is chosen, the NBU for Oracle client must be installed on the backup host, as well as on the primary host.
  - If RMAN sbt_tape backup is chosen, at least one NBU policy of the Oracle type must be created and configured for database backup. Optionally, a separate NBU policy of the Oracle type can be created and configured for archive log backup. See section *4.8 Setting Up NetBackup Policies for Oracle RMAN Backup* on page 4.22 for details.
  - An RMAN Recovery Catalog database must be created and configured prior to using the backup utility.

There are two ways to perform backups:

- Immediate backup - a backup that is initiated by Recovery Manager through the database backup utility.
- Automatic backup - a backup that is initiated by NBU from the NBU master server.

2.10.1.1 Immediate Backup

During an immediate backup, Recovery Manager performs the following:

- Creates an online, offline, datafile, or archonly virtual copy for the database or archive log destination.
- Mounts the virtual copy on the backup host.

For NBU (user-managed) backup, Recovery Manager:

- Generates an include list file that contains a list of datafiles and/or archive log destination on the mounted virtual copy and stores it in the `/usr/openv/netbackup/include_list.<policy_name>` file on the NBU client (the backup host).

- Calls the bpbackup command from the NBU master server to backup files listed in the include list.

For Oracle RMAN backup, Recovery Manager:

- Starts up a clone database in mounted mode using the mounted virtual copy on the backup host, assuming ORACLE_HOME is installed and configured in the Recovery Manager repository.
- Calls an RMAN backup script (`vcdba_rman_dbbackup.sh` or `vcdba_rman_archbackup.sh`) to backup the cloned database.
- Removes the cloned database.
- Un-mounts the virtual copy.

NOTE: The RMAN backup scripts (`vcdba_rman_dbbackup.sh` and `vcdba_rman_archbackup.sh`) are generated at `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>` during the creation of the Recovery Manager Configuration file.

2.10.1.2 Automatic Backup

During an automatic backup, NBU initiates a backup process on the NBU client (the backup host).

For an NBU (user-managed) backup:

- The NBU client executes the `bpstart_notify.<policy_name>` script.
- The `bpstart_notify` script creates a virtual copy of the database or archive log destination, mounts it on the backup host, then generates the include list in the `/usr/openv/netbackup/include_list.<policy_name>` file, which contains a list of files on the virtual copy for backup.
- Once the backup process is completed, the NBU client executes the `bpend_notify.<policy_name>` script to perform virtual copy cleanup.

NOTE: The `bpstart_notify` and `bpend_notify` scripts are generated at `/usr/openv/netbackup/bin` during the creation of the Recovery Manager Configuration file. By default, the `bpstart_notify` script (for database backup policy) will perform an online backup. If an offline or datafile backup is desired, edit this file to set the value of BACKUP_MODE to 'offline' or 'datafile' respectively. In addition, the database must be manually shutdown for offline backup.

For an Oracle RMAN backup:

- The NBU client executes the backup script `vcdba_nbu_dbbackup.sh` or `vcdba_nbu_archbackup.sh`, which must be specified in the Backup Selection List of the NBU policy.
- The backup script creates a virtual copy of the database or archive log destination, mounts it on the backup host, starts up a cloned database in MOUNTED mode, then calls the RMAN backup scripts (`vcdba_rman_dbbackup.sh` or `vcdba_rman_archbackup.sh`) to backup the cloned database.

NOTE: The backup scripts (`vcdba_nbu_dbbackup.sh` and `vcdba_nbu_archbackup.sh`) and the RMAN backup scripts (`vcdba_rman_dbbackup.sh` and `vcdba_rman_archbackup.sh`) are generated at `/etc/3par/solutions/<primary_server>.ora.<oracle_sid>` during the creation of the Recovery Manager Configuration file. By default, the `vcdba_nbu_dbbackup.sh` script (for database backup policy) will perform an online backup. If an offline or datafile backup is desired, edit this file to set the value of BACKUP_MODE to 'offline' or 'datafile' respectively. In addition, the database must be manually put in MOUNTED mode for offline backup.

NOTE: To perform automatic backup, RSH or SSH must have been configured for root user as Veritas NetBackup always initiates a backup as root user.

If the virtual copy is to be backed up using Oracle RMAN, a Recovery Catalog must have been created and configured prior to using the backup utility.

For an RAC database, archive log destinations of all RAC instances must be on shared storage (same cluster file systems or same ASM disk groups).

2.10.2 The Database Restoration Utility

3PAR Recovery Manager's database restoration utility restores databases, tablespaces, datafiles, or archive logs from a virtual copy's backup image. The virtual copy must have been previously backed up using the `vcdba_backup` command. The virtual copy must have a backup status of Y in order to be restored. The virtual copy's backup status can be retrieved using the Recovery Manager display utility (see *2.6.3 The Virtual Copy Display Utility* on page 2.9).

The Recovery Manager restore utility can also be used to restore a virtual copy's backup image to an alternate server. For an NBU (user-managed) restoration, the restore utility can also be used to restore to an alternate location.

The following restrictions apply when restoring from a virtual copy's backup image:

- When restoring the database control file (using the `-c` option) using Oracle RMAN, the database must be in STARTED mode (`startup nomount`). In addition, restoring the database control file along with the individual datafile or tablespace is not supported as it is not possible to perform media recovery.
- When restoring a database, the database must be in CLOSED or MOUNTED mode for NBU restore or Oracle RMAN restore, respectively. For an RAC database, all RAC instances must be in CLOSED or MOUNTED mode.
- When restoring individual tablespaces or datafiles, the database can be OPEN, but the corresponding tablespaces must be offline.
- If the database is an ASM managed database, all ASM disk groups must be mounted prior to running the restore utility.
- For an NBU (user-managed) restoration, the `/usr/openv/netbackup/db/altnames/<database_hostname|virtual _hostname>` file must be created on the NBU master server prior to running the restore utility, where `<database_hostname|virtual_hostname>` is the host name of the database server.

Depending on the type (online, offline, datafile, or archive log) of the virtual copy's backup image, corresponding database files are restored appropriately.

For and NBU (user-managed) restoration:

- Control files are not restored by default.

- For an online virtual copy, both datafiles and archive logs are restored unless individual tablespaces or datafiles are being specified. In this case, only the corresponding datafiles are restored.
- Only datafiles are restored for an offline or datafile virtual copy.
- Only archive logs are restored for an archive log virtual copy.

For an Oracle RMAN restoration:

- Control files are not restored by default.
- For an online virtual copy, only datafiles are restored. Archive logs are not restored to minimize restore time as Oracle RMAN can restore only necessary archive logs during recovery.
- Only datafiles are restored for an offline or datafile virtual copy.
- Restoring from an archive log virtual copy backup image is not supported as Oracle RMAN can restore only necessary archive logs during recovery.

2.11 Recovery Manager with Remote Copy

If 3PAR Remote Copy is set up for a database, 3PAR Recovery Manager’s remote synchronization utility (`vcdba_rsync`) can perform a periodic synchronization of database virtual volumes. Once the synchronization process completes, a virtual copy is created automatically for the remote virtual volumes on the secondary InServ Storage Server. The virtual copy can then be mounted on a backup host for off-host processing purposes.

3
Installing and Deinstalling Recovery Manager

In this chapter

This chapter describes how to install, verify, and remove 3PAR Recovery Manager for Oracle on systems running Linux and Solaris.

3.1 Referencing the Support Matrix

For information about supported platforms, refer to the *InForm OS Configuration Matrix* (part number 320-200099) available from 3PAR's Document Control System.

3.2 Preinstallation Requirements

Recovery Manager must be installed on a primary host and a backup host. The primary host must be running an Oracle10g or above database.

Database backups take place on the backup host that runs Recovery Manager.

Prior to the installation of Recovery Manager, make sure that the following preinstallation requirements are met:

- The same Oracle owner user and Oracle DBA group on the primary (database) server must exist on the backup host. The Oracle owner user ID and Oracle DBA group ID on the backup host must be the same as on the primary host.
- All Oracle data files and archive logs must reside on separate 3PAR virtual volumes.
- Online redo logs and control files can reside on the same virtual volume. However, redo logs and control files must not reside on virtual volumes on which data files and archive logs reside.
- If Veritas Volume Manager is used, the Oracle data files and archive logs must reside on separate VxVM disk groups. Additionally, online redo logs and control files must not reside on VxVM disk groups that are used by Oracle data files and archive logs. The online redo logs and control files can reside on the same VxVM disk group. The primary and backup host must have the same level of operating system patches, Veritas volume manager version, and maintenance patch.
- If ASM is used to manage an Oracle database, Oracle data files and archive logs must reside on different ASM disk groups. Additionally, online redo logs and control files must not reside on ASM disk groups used by Oracle data files and archive logs. The online redo logs and control files can reside on the same ASM disk group.

- If you are using Veritas® NetBackup[1], it is recommended that you use the backup host as the NetBackup master server. The Veritas NetBackup client must be installed on the primary and backup hosts. If you are using Veritas NetBackup in conjunction with Oracle RMAN, the NetBackup for Oracle client must be installed on the primary and backup hosts. Refer to Veritas NetBackup for Oracle for installation and configuration instructions.

  Additionally, you must create an Oracle RMAN Recovery Catalog and configure Oracle TNS Service and Listener to allow connecting to the Recovery Catalog from both the primary and backup hosts. The Recovery Catalog can be created on any host. 3PAR Recovery Manager recommends that the Recovery Catalog is created on the backup host. Refer to Oracle documentation for instructions on how to create a Recovery Catalog, as well as how to configure Oracle TNS Service and Listener.

- Virtual volume snapshots used by an Oracle database must be mapped to a Common Provisioning Group (CPG). Refer to the *3PAR InForm OS CLI Administrator's Manual* for details about mapping to CPGs.

- If you are upgrading from an earlier version of Recovery Manager, you need to uninstall the earlier version of Recovery Manager first as a root user before installing the newer version.

- Refer to 3PAR Implementation Guides for instructions on setting up connections from hosts to the InServ Storage Server and reserving LUNs with specific Host Bus Adapters (HBAs).

- Recovery Manager's Remote Copy feature only supports periodic synchronization with 1 to 1 topology. To use the Remote Copy feature, you must configure your InServ Storage Servers for Remote Copy. The InServ Storage Servers must meet the requirements specified in *9.2.1 Recovery Manager's Remote Copy Requirements* on page 9.3. For instructions on configuring storage servers for Remote Copy, see the *3PAR Remote Copy User's Guide.*

- (Solaris only) If a trusted host connection (RSH) is to be used, the InForm OS Command Line Interface (CLI) must be installed to the `/opt/3par/cli` directory prior to installing Recovery Manager.

- If a secure shell (SSH) connection is to be used, see Chapter 4, *Configuring Recovery Manager*.

[1] Veritas NetBackup is third-party software, and 3PAR makes no representations or warranties with respect to such software.

3.3 Installing Recovery Manager on Linux Systems

Use the instructions in this section to install 3PAR Recovery Manager software on both the primary and backup hosts.

3.3.1 Starting Installation

The following section describes the steps necessary for installing 3PAR Recovery Manager on a Linux system:

CAUTION: When upgrading to a newer version of 3PAR Recovery Manager, any previously installed versions of Recovery Manager must be removed. Use the `rpm -e VCDBAora` command to remove the previously installed package.

To install 3PAR Recovery Manager:

1 Log in as the `root` user.

2 Insert the 3PAR Recovery Manager CD into a CD-ROM drive.

NOTE: If the CD is not mounted automatically, you can mount it manually.

```
# mount -t iso9660 -r /dev/cdrom /mnt/cdrom
```

3 Change to the CD-ROM drive.

```
# cd /mnt/cdrom0
```

4 Issue the `rpm` command as follows:

```
# rpm –ihv –-percent -–nodeps VCDBAora-302-1.i386.rpm
```

3.3.2 Verifying Installation

To verify 3PAR Recovery Manager installation on a Linux system:

1. Log in as the `root` user.
2. Issue the `rpm` command as follows:

```
# rpm -qi VCDBAora

Name        : VCDBAora                     Relocations: (not relocatable)
Version     : 302                          Vendor: 3PAR, Inc.
Release     : 1                             Build Date: Thu 18 Sep 2008 05:28:57
PM PDT
Install Date: Fri 19 Sep 2008 03:49:59 PM PDT      Build Host: spinner
Group       : Applications/system           Source RPM: VCDBAora-302-1.src.rpm
Size        : 112747698                        License: 3PAR, Inc.
Signature   : (none)
Packager    : John Smith <johnsmith@3par.com>
Summary     : Recovery Manager for Oracle on Linux
Description :
3PAR Recovery Manager for Oracle on Linux, it provides a set of utilities to
perform 3PAR Virtual Copy administration for online backup, restore and off-host
processing.
```

3. After the installation is complete on the primary and backup hosts, you can allow Oracle users and Database Administrators group access to the Recovery Manager commands and utilities by changing the owner and permissions of the following directories (required for Oracle users):

   - `/opt/3par/vcdbaora`
   - `/etc/3par/solutions`
   - `/etc/3par/solutions/log`
   - `/etc/3par/solutions/lock`
   - `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>`

a. Change the owner of the Recovery Manager utilities and repository as follows, where the Database Administrator user name is <user> and the group name is <group>:

```
#chown <user>:<group> /opt/3par/vcdbaora
#chown <user>:<group> /etc/3par/solutions
#chown <user>:<group> /etc/3par/solutions/log
#chown <user>:<group> /etc/3par/solutions/lock
```

b. Change the access permission of the Recovery Manager utilities as follows:

```
#chmod 550 /opt/3par/vcdbaora
```

4. If the `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>` directory exists, you must also change the owner and permission as follows:

```
# chown -R <user>:<group> /etc/3par/solutions/
<primary_host>.ora.<oracle_sid>
```

3.4 Removing Recovery Manager from Linux Systems

To deinstall 3PAR Recovery Manager from a Linux system:

1. Log on as the `root` user.

2. Use the rpm command as follows:

```
# rpm -e VCDBAora
```

3.5 Installing Recovery Manager on Solaris Systems

Use the instructions in this section to install 3PAR Recovery Manager software on both the primary and the backup hosts.

CAUTION: Prior to upgrading to 3PAR Recovery Manager, deinstall any previously installed versions of Recovery Manager. To remove a previously installed package, log on as the `root` user and use the `pkgrm VCDBAora` command.

3.5.1 Starting Installation

To install 3PAR Recovery Manager on a Solaris system:

1. Log on as the root user.
2. Insert the 3PAR Recovery Manager CD into a CD-ROM drive.

   If the CD is not mounted automatically, you will need to mount it manually.

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2/cdrom
```

3. Change to the CD-ROM drive.

```
# cd /cdrom/cdrom0
```

4. Use the pkgadd command as follows:

```
# pkgadd -d . VCDBAora
```

   You will be prompted to answer several questions about creating the installation area and the setuid files to be installed.

NOTE: Install the following two patches if applicable:

- Solaris 5.9 SSH requires patch 114356-05, or higher.
- Solaris 5.10 requires patch 119130-26, or higher.

The following commands can be used to verify whether the patches are installed or not:

- `showrev -p | grep 114356`
- `showrev -p | grep 119130`

3.5.2 Verifying Installation

To verify 3PAR Recovery Manager installation on a Solaris system:

1. Log in as the root user.

2 Use the pkginfo command as follows:

```
# pkginfo -l VCDBAora
PKGINST:  VCDBAora
      NAME:  3PAR Recovery Manager for Oracle on Solaris
  CATEGORY:  application
      ARCH:  Sparc
   VERSION:  3.0.2
   BASEDIR:  /opt/3par/vcdbaora
    VENDOR:  3PAR
      DESC:  3PAR Recovery Manager for Oracle on Solaris
    PSTAMP:  vcdbaora-3.0.2: 01-19-2007 15:07:30
  INSTDATE:  Jan 19 2007 15:21
 HOTLINE:  1-510-413-5999
     EMAIL:  salesinfo@3pardata.com
    STATUS:  completely installed
     FILES:      106 installed pathnames
                   7 shared pathnames
                  21 directories
                  50 executables
                   4 setuid/setgid executables
              166294 blocks used (approx)
```

3 After the installation is complete on the primary and backup hosts, you can allow Oracle users and Database Administrators group access to the Recovery Manager commands and utilities by changing the owner and permissions of the following directories (required for Oracle users):

- /opt/3par/vcdbaora
- /etc/3par/solutions
- /etc/3par/solutions/log
- /etc/3par/solutions/lock
- /etc/3par/solutions/<primary_host>.ora.<oracle_sid>

a Change the owner of the Recovery Manager utilities and repository as follows, where the Database Administrator user name is <user> and the group name is <group>:

```
#chown <user>:<group> /opt/3par/vcdbaora
#chown <user>:<group> /etc/3par/solutions
#chown <user>:<group> /etc/3par/solutions/log
#chown <user>:<group> /etc/3par/solutions/lock
```

b Change the access permission of the Recovery Manager utilities as follows:

```
#chmod 550 /opt/3par/vcdbaora
```

4 If the /etc/3par/solutions/<primary_host>.ora.<oracle_sid> directory exists, you must also change the owner and permission as follows:

```
# chown -R <user>:<group> /etc/3par/solutions/
<primary_host>.ora.<oracle_sid>
```

3.6 Removing Recovery Manager from Solaris Systems

To remove 3PAR Recovery Manager from a Solaris system:

1 Log in as the root user.

2 Use the pkgrm command as follows:

```
# pkgrm VCDBAora
```

3.10 Removing Recovery Manager from Solaris Systems

4
Configuring Recovery Manager

In this chapter

4.1 Setting Up Connections on Recovery Manager

3PAR Recovery Manager requires that either an RSH/CLI or SSH connection be configured for the backup host, the primary host, the Veritas NetBackup master server, and the InServ Storage Server.

NOTE: RSH connection is available for Solaris systems only.

Since Recovery Manager can be run by either the root user or Oracle user (Oracle owner), perform one of the following:

- For Solaris systems, configure RSH or SSH for the root or Oracle user.
- For Linux systems, configure SSH for the root or Oracle user.

NOTE: RSH or SSH must be set up for the root user in order to use Veritas NetBackup's automatic backup feature (a back up initiated from the NetBackup master server), as NetBackup always initiates a backup as the root user.

The following sections describe how to set up RSH and SSH connections.

4.2 Setting up RSH/CLI Connections for Recovery Manager

NOTE: RSH connections are available for Solaris systems only.

This section describes how to set up RSH/CLI for a root user on the primary host, backup host, Veritas NetBackup master server, and the InServ Storage Server.

NOTE: If you are setting up an RSH connection, you must install the 3PAR InForm Command Line Interface (CLI) in the `/opt/3par/cli` directory prior to installing 3PAR Recovery Manager. Refer to the *InForm OS CLI Administrator's Manual* for instructions on installing the InForm CLI.

Figure 4-1 represents the RSH/CLI connections relationship between the primary host, the backup host, Veritas NetBackup master server, and the InServ Storage Server.

Figure 4-2 represents the RSH/CLI connection relationship with 3PAR Remote Copy support.

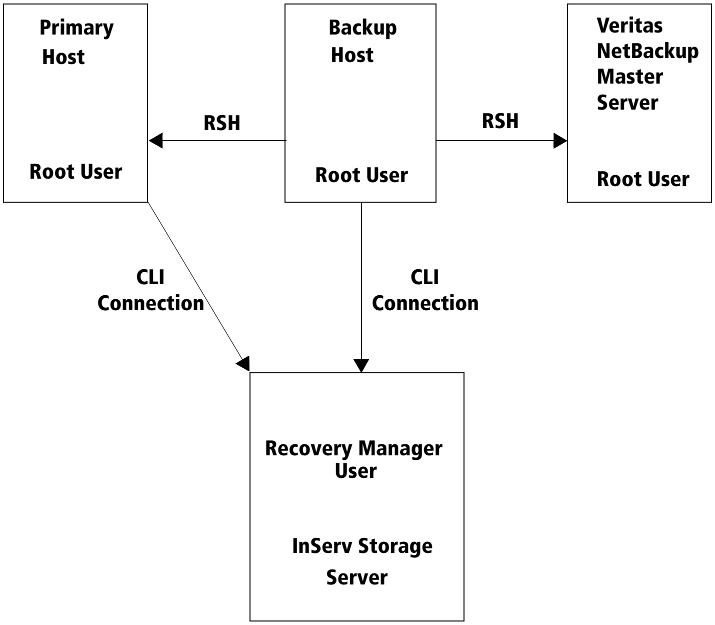


Figure 4-1. RSH/CLI Connection Relationship

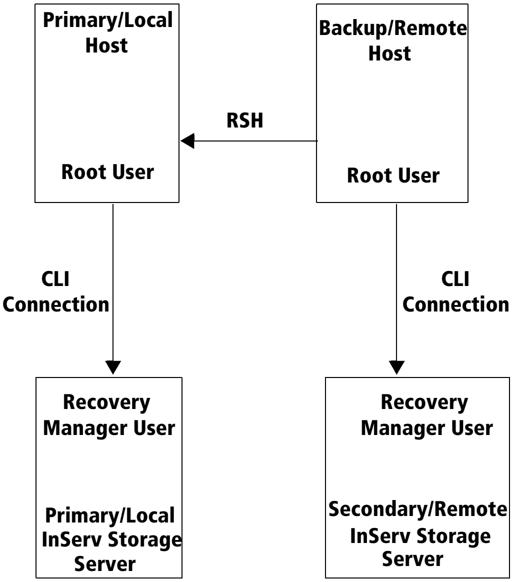


Figure 4-2. RSH/CLI Connection Relationship for Remote Copy Support

4.2.1 Setting Up an RSH Connection from the Backup Host to the Primary Host

To set up an RSH connection from the backup host to the primary host:

1 Log in to the primary host as the `root` or Oracle user.

2 Modify or create the `~/.rhosts` file to contain the following lines:

```
<backup_host> <user>
```

where:

- `<backup_host>` is the host name of the backup host.
- `<user>` is the root user name on the backup host.

4.2.2 Verifying the RSH Connection from the Backup Host to the Primary Host

From the backup host, verify the RSH connection to the primary host as follows:

1 On the backup host, login in as the root or Oracle user (as you logged in during set up).

2. Issue the `rsh` command for the primary host as follows:

```
<backup_host># rsh <primary_host> ls /
```

3. Make sure the command completes successfully.

4.2.3 Setting Up RSH Connections from the Backup Host to the NetBackup Master Server

If the Veritas NetBackup master server and the Recovery Manager backup host are not the same, you must set up the RSH connection to the NetBackup master server as described in the following steps. Otherwise, skip this section.

To set up an RSH connection from the backup host to the Veritas NetBackup master server:

1. Log in to the NetBackup master server as the `root` or Oracle user.
2. Modify or create the `~/.rhosts` file to contain the following line:

```
<backup_host> <root_user>
```

where:

- `<backup_host>` is the host name of the backup host.
- `<root_user>` is the root user's name on the backup host.

4.2.4 Verifying RSH Connections from the Backup Host to the NetBackup Master Server

From the backup host, verify the RSH connection to the NetBackup master server as follows:

1. On the backup host, login in as the root or Oracle user (as you logged in during set up).
2. Issue the `rsh` command for the NetBackup master server as follows:

```
<backup_host># rsh <nbu_master> ls /
```

Make sure the command completes successfully.

4.2.5 Setting Up a CLI Connection from the Primary Host to the InServ Storage Server

Set up a CLI connection from the primary host to the InServ Storage Server as follows:

1 On the primary host, set the environment variables as follows:

```
#TPDSYSNAME=<ss_name>
#TPDPWFILE=<ss_pwfile>
#export TPDSYSNAME TPDPWFILE
```

where:

- `<ss_name>` is the system name of the InServ Storage Server attached to the primary host.
- `<ss_pwfile>` is the location for the InServ Storage Server user password file.

NOTE: Before creating a CLI user, refer to the *InForm OS CLI Administrator’s Manual* for a list of reserved user names.

2 On the primary host, create a CLI user as follows:

```
<primary_host># /opt/3par/cli/bin/createuser -c \
<password> <username> all edit
```

where `<username>` is the name of the user being created.

For additional information about the `createuser` command, see the *InForm OS Command Line Interface Reference*.

3 On the primary host, create a storage server user password file as follows:

```
<primary_host># /opt/3par/cli/bin/setpassword -saveonly -file \
$TPDPWFILE -u <username>
```

where <username> is the username you created in step 2.

4.2.6 Verifying the CLI Connection from the Primary Host to the InServ Storage Server

From the primary host, verify the CLI connection to the InServ Storage Server as follows:

1. On the primary host, log in as the root or Oracle user (as you logged in during set up).
2. Issue any CLI command (such as `showsys`) and ensure that the command completes successfully.

```
<primary_host># showsys
```

4.2.7 Setting Up a CLI Connection from the Backup Host to the InServ Storage Server

Set up a CLI connection from the backup host to the InServ Storage Server as follows:

1. On the backup host, set the environment variables as follows:

```
#TPDSYSNAME=<ss_name>
#TPDPWFILE=<ss_pwfile>
#export TPDSYSNAME TPDPWFILE
```

where:

- `<ss_name>` is the system name of the InServ Storage Server attached to the backup host.
- `<ss_pwfile>` is the location for the InServ Storage Server user password file.

NOTE: The following step is optional. Perform step 2 if you want 3PAR Recovery Manager to access the InServ Storage Server from the backup host as a different user than the user created on the primary host.

2. On the backup host, create a CLI user on the InServ Storage Server as follows:

```
<backup_host># /opt/3par/cli/bin/createuser -c \<password> <username> all
edit
```

See the *InForm OS Command Line Interface Reference* for additional information on the `createuser` command.

3. On the backup host, create a storage server user password file as follows:

```
<backup_host># /opt/3par/cli/bin/setpassword -saveonly -file \
$TPDPWFILE -u <username>
```

   where <username> is the name of the user you created in step 2 in this section or in *4.2.2 Verifying the RSH Connection from the Backup Host to the Primary Host* on page 4.4.

4.2.8 Verifying the CLI Connection from the Backup Host to the InServ Storage Server

From the backup host, verify the CLI connection to the InServ Storage Server as follows:

1. On the backup host, log in as the root or Oracle user (as you logged in during set up).
2. Issue any CLI command (such as `showsys`) and ensure that the command completes successfully.

```
<backup_host># showsys
```

4.3 Setting Up SSH Connections for Recovery Manager

This section provides instructions on how to configure a Secure Shell (SSH) connection for the root user on the primary host, backup host, NetBackup (NBU) master server, and the InServ Storage Server.

Figure 4-3 represents the SSH connection relationship between the primary host, the backup host, and the InServ Storage Server.

Figure 4-4 represents the SSH connection relationship in a Remote Copy configuration.

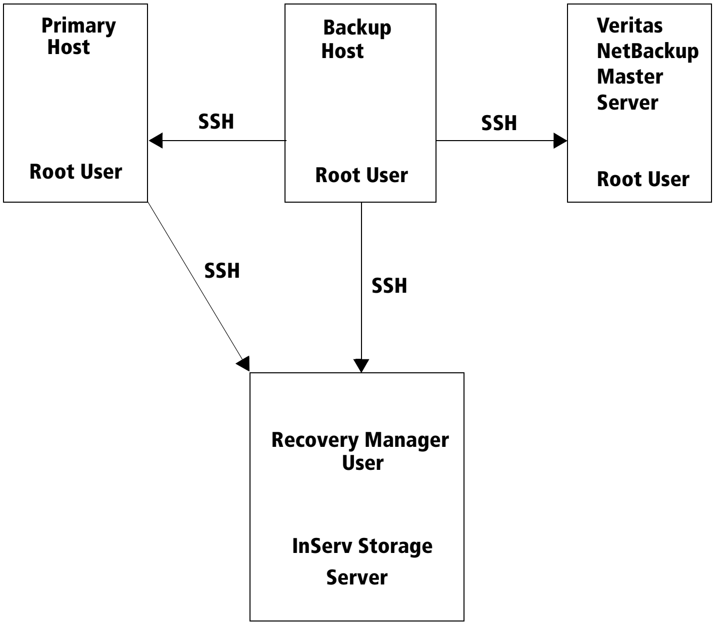


Figure 4-3. SSH Connection Relationship

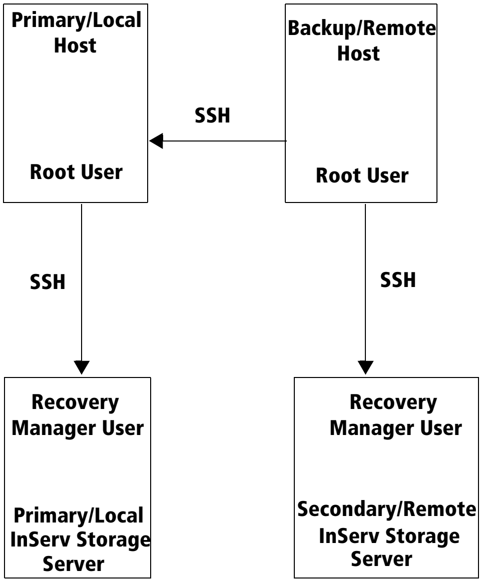


Figure 4-4. SSH Connection Relationship for Remote Copy Support

4.3.1 SSH Restrictions

Recovery Manager has the following SSH restrictions:

- The `ssh` and `scp` commands must be located in the `/usr/bin/` directory. Create symbolic links as follows:

```
#ln -s /usr/local/bin/ssh /usr/bin/ssh
#ln -s /usr/local/bin/scp /usr/bin/scp
```

- SSH keys on the primary and backup hosts must be generated with no passphrase. Recovery Manager does not support an SSH passphrase or SSH agent.

4.3.2 Modifying the SSH Daemon Configuration

If SSH needs to be configured for the root user, then the SSH daemon on the primary host, backup host, and NetBackup master server must be configured to allow root access. Perform the following on each system:

1. Verify that the SSH daemon allows root access by checking the `sshd_config` file for the following line:

```
PermitRootLogin yes
```

NOTE: If you are using native SSH, the sshd_config file is located in `/etc/ssh/sshd_config`.

2 If the line reads `PermitRootLogin no`, change the line to read `yes`.

4.3.3 Generating an SSH Key Pair for the Backup Host

To generate an SSH key pair for the backup host:

1 Log on to the backup host as the `root` user.

2 Create a key pair with no passphrase using the `ssh-keygen` command. If a key-pair already exists, skip this section.

```
<backup_host:# ssh-keygen -b 1024 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (//.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in //.ssh/id_rsa.
Your public key has been saved in //.ssh/id_rsa.pub.
The key fingerprint is:
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx root@<backup_host>
```

NOTE: You can create the SSH key as either `dsa` or `rsa`. The recommended key length is 1024 (the total of the public and private key lengths).

The `ssh-keygen` utility generates two files, `id_rsa` and `id_rsa.pub` (or `id_dsa` and `id_dsa.pub`). The `id_rsa` (or `id_dsa`) file contains the private key and the `id_rsa.pub` (or `id_dsa.pub`) file contains the public key.

4.3.4 Generating an SSH Key Pair for the Primary Host

You can either use the same SSH key pair generated for the backup host or generate a different SSH key pair for the primary host. If you choose to use the same key pair, create one InForm CLI user, otherwise, create two different CLI users to be accessed from the primary host and the backup host, respectively. If you are generating a different SSH key pair for the primary host, perform the procedure described in *4.3.3 Generating an SSH Key Pair for the Backup Host* on page 4.11 on the primary host.

NOTE: In an RAC environment, all the nodes in the cluster must have the same SSH key pair in order to run Recovery Manager utilities against any RAC instance on any node.

If you choose to use the same SSH key pair, create one InForm CLI user (see *4.3.7 Setting Up Connections from the Backup Host to the NetBackup Master Server* on page 4.13 and *4.3.9 Setting Up Connections from the Backup Host to the InServ Storage Server* on page 4.14). Then copy the SSH key pair from the backup host to the primary host as follows:

```
<primary_host> # scp <backup_host>:~/.ssh/* ~/.ssh
The authenticity of host 'pilot (192.168.3.130)' can't be established.
RSA key finger print is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'pilot (192.168.3.130)' to the list of known
hosts.
root@pilot's password:
```

4.3.5 Setting Up Connections from the Backup Host to the Primary Host

To set up an SSH connection from the backup host to the primary host, perform the following:

- Copy the public key (`id_rsa`.pub) of the backup host to the `authorized`_keys file of the primary host.

```
<backup_host> # scp ~/.ssh/id_rsa.pub <primary_host>:~/.ssh/authorized_keys
```

If the `authorized`_keys file already exist, add the public key to the end of the authorized_keys file.

4.3.6 Verifying Connections from the Backup Host to the Primary Host

From the backup host, verify the connection to the primary host as follows:

NOTE: If you are prompted for a password, the setup is incorrect and you must redo the previous setup.

```
<backup_host># ssh root@<primary_host>
              The authenticity of host '<primary_host>' can't be established.
              DSS key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:x:xx:xx.
              Are you sure you want to continue connecting (yes/no)? yes

              Warning: Permanently added '<primary_host>' (DSS) to the list of
              known hosts.
```

where `<primary_host>` is the primary host's hostname.

4.3.7 Setting Up Connections from the Backup Host to the NetBackup Master Server

To set up an SSH connection from the backup host to the NetBackup (NBU) master server, perform the following:

- Copy the public key (`id_rsa.pub`) of the backup host to the `authorized_keys` file of the NBU master server.

```
<backup_host # scp ~/.ssh/id_rsa.pub <NBU_server>:~/.ssh/authorized_keys
```

If the `authorized_keys` file already exist, add the public key to the end of the `authorized_keys` file.

4.3.8 Verifying Connections from the Backup Host to the NetBackup Master Server

From the backup host, verify the connection to the NetBackup master server as follows:

NOTE: If you are prompted for a password, the setup is incorrect and you must redo the previous setup.

```
<backup_host># ssh root@<NBU_master>
              The authenticity of host '<NBU_master>' can't be established.
              DSS key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:x:xx:xx.
              Are you sure you want to continue connecting (yes/no)? yes

              Warning: Permanently added '<NBU_master>' (DSS) to the list of
              known hosts.
```

4.3.9 Setting Up Connections from the Backup Host to the InServ Storage Server

Set up an SSH connection from the backup host to the InServ Storage Server as follows:

1 Log in to the backup host as root user.

2 Make sure the SSH key pair exists as follows:

```
<backup_host> # ls ~/.ssh
id_rsa id_rsa.pub authorized_keys known_hosts
```

3 Create a CLI user on the InServ Storage Server to be used by 3PAR Recovery Manager to access the InServ Storage Server from the backup host. Skip this step if you wish to use an existing user.

```
<backup_host># ssh <adm_user>@<ss_name>
<adm_user>'s password: <adm_password>
cli% createuser -c <password> <username> all edit
```

In the example above:

- <adm_user> is the user name of the InServ Storage Server’s administrator.
- <ss_name> is the system name of the InServ Storage Server attached to the backup host.
- <adm_password> is the administrator's password.
- <password> is the password (for the InServ Storage Server) for the CLI user being created.
- <username> is the user being created.

For details about the `createuser` command, refer to the *InForm OS Command Line Interface Reference*.

4 Copy the public key of the backup host to the InServ Storage Server.

```
<backup_host># ssh <username>@<ss_name>
<username>'s password: <password>

cli% setsshkey
Please enter the SSH puplic key below. When finished, press enter twice. The
key is usually long. It's better to copy it from inside and editor and paste
it here. (Please make sure there are no extra blanks.)

<pass the public key here and press Enter twice>

<public_key>

SSH public key successfully set!
```

In the example above:

- `<username>` is the user being created.
- `<ss_name>` is the system name of the InServ Storage Server attached to the backup host.
- `<password>` is the password for the CLI user being created.
- `<public_key>` is the SSH public key of the backup host.

4.3.10 Verifying Connections from the Backup Host to the InServ Storage Server

From the backup host, verify the connection from the backup host to the InServ Storage Server as follows:

> **NOTE:** If you are prompted for a password, the setup is incorrect and you must redo the previous setup.

```
<backup_host># ssh <username>@<ss_name>
         The authenticity of host '<ss_name>' can't be established.
         DSS key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:x:xx:xx.
         Are you sure you want to continue connecting (yes/no)? yes

         Warning: Permanently added '<InServ_name>' (DSS) to the list of
         known hosts.
```

where:

- <user_name> is the CLI user created in *4.3.7 Setting Up Connections from the Backup Host to the NetBackup Master Server* on page 4.13.
- <ss_name> is the system name of the InServ Storage Server attached to the backup host.

4.3.11 Setting Connections from the Primary Host to the InServ Storage Server

Skip this step if the primary host has the same SSH key pair as the SSH key pair of the backup host (see *4.3.4 Generating an SSH Key Pair for the Primary Host* on page 4.11). 3PAR Recovery Manager uses the same CLI user to access the InServ Storage Server from either the backup host or primary host.

If you created a different CLI user for the primary host, perform the following to set up an SSH connection from the primary host to the InServ Storage Server.

1. Log in to the primary host as root user.
2. Make sure the SSH key pair exists as follows:

```
<primary_host> # ls ~/.ssh
id_rsa id_rsa.pub authorized_keys known_hosts
```

3. Create a CLI user to be used by Recovery Manager to access the InServ Storage Server from the primary host. Skip this step if you wish to use an existing user (different from the user created for the backup host).

```
<primary_host># ssh <adm_user>@<ss_name>
<adm_user>'s password: <adm_password>
cli% createuser -c <password> <username> all edit
```

In the example above:

- <adm_user> is the user name of the InServ Storage Server’s administrator.
- <ss_name> is the system name of the InServ Storage Server attached to the primary host.
- <adm_password> is the administrator's password.
- <password> is the password (for the InForm Storage Server) for the CLI user being created.
- <username> is the user being created.

4 Copy the public key of the primary host to the InServ Storage Server.

```
<primary_host># ssh <username>@<ss_name>
<username>'s password: <password>

cli% setsshkey
Please enter the SSH puplic key below. When finished, press enter twice. The
key is usually long. It's better to copy it from inside and editor and paste
it here. (Please make sure there are no extra blanks.)

<pass the public key here and press Enter twice>

<public_key>

SSH public key successfully set!
```

In the example above:

- <username> is the user being created.
- <ss_name> is the system name of the InServ Storage Server attached to the primary host.
- <password> is the password for the CLI user being created.
- <public_key> is the SSH public key of the primary host.

4.3.12 Verifying Connections from the Primary Host to the InServ Storage Server

From the primary host, verify the connection from the primary host to the InServ Storage Server as follows:

NOTE: If you are prompted for a password, the setup is incorrect and you must redo the previous setup.

```
<primary_host># ssh <username>@<ss_name>
         The authenticity of host '<ss_name>' can't be established.
         DSS key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:x:xx:xx.
         Are you sure you want to continue connecting (yes/no)? yes

         Warning: Permanently added '<ss_name>' (DSS) to the list of
         known hosts.
```

where:

- `<username>` is the CLI user created in *4.3.9 Setting Up Connections from the Backup Host to the InServ Storage Server* on page 4.14.
- `<ss_name>` is the name of the InServ Storage Server attached to the primary host.

4.4 Setting up National Language Host Support

The 3PAR Recovery Manager message catalog is installed in the `/opt/3par/vcdbaora/msg/en_US` directory and the symbolic link is installed in the `/usr/lib/locale/en_US` directory.

- To retrieve the text messages properly, you must set the NLSPATH path environment.

```
# NLSPATH=$NLSPATH:/usr/lib/locale/%L/%N

# export NLSPATH
```

4.5 Setting up Manual Pages on Both Primary and Backup Hosts

3PAR Recovery Manager provides manual pages in the /opt/3par/vcdbaora/man directory.

- To access the manual pages, define the environment variable MANPATH as follows:

```
# MANPATH=$MANPATH:/opt/3par/vcdbaora/man
# export MANPATH
# LC_ALL=en_US
#export LC_ALL
```

4.6 Setting up a Search Path on Both Primary and Backup Hosts

3PAR Recovery Manager executables are stored in the /opt/3par/vcdbaora/bin directory is provided for main programs.

- To add the Recovery Manager executables to the Recovery Manager search path, use the following commands:

```
# PATH=$PATH:/opt/3par/vcdbaora/bin

# export PATH
```

4.7 Setting Up NetBackup Policies for NBU (User-Managed) Backup

3PAR Recovery Manager supports NetBackup (NBU) with or without RMAN. The following sections describe how to set up NBU policies for NBU backup without RMAN.

Recovery Manager supports full, incremental, or cumulative incremental archive log backup (backup only archive logs). When performing NBU backup without RMAN, Recovery Manager supports only full database backup (incremental database backup is not possible). However, you can combine full database backup with archive log backup to simulate incremental database backup.

Recovery Manager requires that you create an NBU policy for database backup. If you wish to perform archive log backup, you must create a separate NBU policy for it.

NOTE: This section assumes that you are familiar with the Oracle Database and Veritas NetBackup (NBU). For more information on creating a NetBackup policy, refer to Veritas NetBackup documentation.

4.7.1 Configuring the NetBackup Policy for Database Backup

For 3PAR Recovery Manager to perform backup and restoration correctly, you must use the following guidelines in conjunction with Veritas NetBackup documentation when configuring a NBU policy:

Backup Attribute	1 Select the standard type for the policy. 2 Select the **cross mount points** option. 3 Deselect the **Allow multiple data stream** and **Block level incremental** options.
Backup Selections	1 It is recommended that you enter `/dummy` for the backup selections. 2 Recovery Manager generates the backup selection list on the fly to replace the value you entered.
Backup Schedule	1 Create a schedule for full backup. 2 If you wish to perform immediate database backup (initiated from Recovery Manager), set the backup window to **0**. 3 If you also wish to perform automatic database backup (initiated from NBU), specify the backup window to fit your needs.
Backup Clients	Set the backup client to the host name of the backup host, as the backup process will actually take place on the backup host.

4.7.2 Configuring the NetBackup Policy for Archive Log Backup

Perform this step only if you want to only backup the archive logs. For Recovery Manager to perform backup and restoration correctly, you must use the following guidelines in conjunction with Veritas NetBackup documentation when configuring a NBU policy:

Backup Attribute	1 Select the standard type for the policy. 2 Select the **cross mount points** option. 3 Deselect the **Allow multiple data stream** and **Block level incremental** options.
Backup Selections	1 It is recommended that you enter `/dummy` for the backup selections. 2 Recovery Manager generates the backup selection list on the fly to replace the value you entered.
Backup Schedule	1 Create two schedules, one for full backup and one for incremental backup (optional). For the incremental backup schedule, you can create either a differential incremental or cumulative incremental backup schedule. 2 If you wish to perform immediate archive log backup (initiated from Recovery Manager), set the backup window to **0**. 3 If you also wish to perform automatic archive log backup (initiated from NBU), specify the backup window to fit your needs.
Backup Clients	Set the backup client to the host name of the backup host, as the backup process will actually take place on the backup host.

4.7.3 Setting Up NetBackup Configuration Parameters

For Recovery Manager to perform backups correctly, the following parameters in the `/usr/openv/netbackup/bp.conf` file must be changed on the backup host (NBU client). If a virtual hostname is used on the primary host for cluster purposes, the CLIENT_NAME must be specified in the `bp.conf` file for the virtual hostname in order for the Recovery Manager restoration utilitiy to function properly.

- `USE_CTIME_FOR_INCREMENTAL`
- `BPSTART_TIMEOUT = 600`
- `BPEND_TIMEOUT = 600`
- `CLIENT_NAME = <virtual_hostname>`

4.8 Setting Up NetBackup Policies for Oracle RMAN Backup

The following sections describe how to set up NetBackup (NBU) policies for NBU backup with RMAN.

To perform NBU backup with RMAN, you must have Veritas NetBackup for Oracle installed on the NBU master server, VERTIAS NetBackup client for Oracle installed on the primary host and the backup host. Refer to Veritas NetBackup for Oracle for installation and configuration instructions.

In addition, you must create an Oracle RMAN Recovery Catalog and configure Oracle TNS Service and Listener to allow connections to the Recovery Catalog from both primary and backup host. The Recovery Catalog can be created on any server. 3PAR Recovery Manager recommends that the Recovery Catalog is created on the backup host. See *4.8.3 Creating an RMAN Recovery Catalog* on page 4.24 for instructions.

When perform NBU backup with RMAN, Recovery Manager supports full, differential, and cumulative incremental database backup. Recovery Manager also support full archive log backup (backup only archive logs).

Recovery Manager requires that you create a NBU policy for database backup. If you wish to perform archive log backup, you must create a separate NBU policy for it.

NOTE: This section assumes that you are familiar with Oracle Database and Veritas NetBackup (NBU). For more information on how to create NetBackup policy, refer to Veritas NetBackup for Oracle documentation.

4.8.1 Configuring the NetBackup Policy for Database Backup with RMAN

For Recovery Manager to perform backup and restoration correctly, you must use the following guidelines in conjunction with Veritas NetBackup documentation when configuring a NBU policy:

Backup Attribute	Select the Oracle type for the policy.
Backup Selections	1 Enter the location of RMAN backup script (`/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/vcdba_nbu_dbbackup.sh`). 2 Recovery Manager will generate the RMAN backup script at the specified location when you create the configuration file (see *4.9 Recovery Manager Configuration Files* on page 4.27 below for details).
Backup Schedule	1 Create two schedules, one for full backup and one for incremental backup (optional). For the incremental backup schedule, you can create either a differential incremental or cumulative incremental backup schedule. 2 If you wish to perform immediate database backup (initiated from Recovery Manager), set the backup window to **0**. 3 If you also wish to perform automatic database backup (initiated from NBU), specify the backup window to fit your needs.
Backup Clients	Set the backup client to the host name of the backup host, as the backup process will actually take place on the backup host.

4.8.2 Configuring the NetBackup Policy for Archive Log Backup

Perform this step only if you wish to backup only archive logs. For Recovery Manager to perform backup and restoration correctly, you must use the following guidelines in conjunction with Veritas NetBackup documentation when configuring a NBU policy:

Backup Attribute	Select the Oracle type for the policy.
Backup Selections	1 Enter the location of RMAN backup script (`/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/vcdba_nbu_archbackup.sh`). 2 Recovery Manager will generate the RMAN backup script at the specified location when you create the configuration file (see *4.9 Recovery Manager Configuration Files* on page 4.27 below for details).
Backup Schedule	1 Create a schedule for full backup. 2 If you wish to perform immediate archive log backup (initiated from Recovery Manager), set the backup window to **0**. 3 If you also wish to perform automatic archive log backup (initiated from NBU), specify the backup window to fit your needs.
Backup Clients	Set the backup client to the host name of the backup host, as the backup process will actually take place on the backup host.

4.8.3 Creating an RMAN Recovery Catalog

This section describes how to create and configure an RMAN Recovery Catalog. Refer to Oracle documentation for more detailed information.

1. Create a database for housing the Recovery Catalog. Oracle suggests the following disk space requirements:

   - System tablespace: 100 MB
   - Temp tablespace: 5 MB
   - Rollback segment: 5 MB
   - Online redo log: 1 MB (each)
   - Recovery Catalog: 10 MB

2 Create a tablespace for the Recovery Catalog as follows:

```
$ export ORACLE_SID=<catdb>
$ export ORACLE_HOME=<oracle_home>
$ sqlplus "/as sysdba"
SQL> create tablespace <cat_tbs> datafile '<path/filename>' size 10M;
SQL> exit
```

where:

- `<catdb>` is the Oracle Instance ID of the Recovery Catalog.
- `<cat_tbs>` is the Recovery Catalog tablespace name.
- `<path/filename>` is the file path where the datafile is created.

3 Create a user for the Recovery Catalog as follows:

```
$ sqlplus "/as sysdba"
SQL> create user <rman_user> identified by <rman_password>
           temporary tablespace temp
           default tablespace <cat_tbs>
           quota unlimited on <cat_tbs>;
SQL> grant connect, resource, recovery_catalog_owner to <rman_user>;
```

where:

- `<tbs_name>` is the tablespace name of the Recovery Catalog.
- `<rman_user>` is the user name to be granted access permission to the Recovery Catalog.
- `<rman_password>` is the password for the `<rman_user>`.

4 Create the RMAN Recovery Catalog tables as follows:

```
$ rman catalog <rman_user>/<rman_password>@<catdb>
RMAN> create catalog tablespace <cat_tbs>;
```

5. Configure TNS services for the Recovery Catalog database by adding an entry in the `$ORACLE_HOME/network/admin/tnsnames.ora` file on the primary host and backup host as follows:

```
<catdb > =
  (description =
    (address = (protocol = TCP) (host = <cat_host>) (port = 1521))
    (connect_data = (server = dedicated) (service_name = <catdb>))
  )
```

   where `<cat_host>` is the host name of the host where the catalog is created.

6. Configure the Oracle listener for the Recovery Catalog database by adding an entry in the `$ORACLE_HOME/network/admin/listener.ora` file on the host where the Recover Catalog is created as follows:

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = <catdb>)
      (ORACLE_HOME = <oracle_home>)
      (SID_NAME = <catdb>)
    )
  )
```

7. Log in as the Oracle owner user and register the database on the primary host.

```
$ rman target / catalog <rman_user>/<rman_password>@<catdb>
RMAN> register database;
```

4.9 Recovery Manager Configuration Files

The following section provides instructions on creating Recovery Manager configuration files.

There are two types of configuration files for Recovery Manager:

- Recovery Manager without Remote Copy support.

  For this type of configuration, Recovery Manager provides an integrated Veritas NetBackup and Oracle RMAN for backups and restorations.

- Recovery Manager with Remote Copy.

  For this type of configuration, Recovery Manager does not provide tools for media backups and restorations.

You can choose to create the Recovery Manager configuration file by either using the Command Line Interface (CLI), menu-driven application, or a Graphical User Interface (GUI).

NOTE: New features are no longer being added to the menu-driven application.

4.9.1 Creating a Recovery Manager Configuration File without Remote Copy

The configuration file can be created in the following ways:

- Menu-driven application
- CLI
- GUI

4.9.1.1 Creating Configuration Files using the Menu-Driven Application or the Command Line Interface on the Backup Host

To create a Recovery Manager configuration file without Remote Copy support:

1 From the backup host, start Recovery Manager.

```
<backup host># opt/3par/vcdbaora/bin/vcdba_main
```

2 If you are using the CLI, from the backup host, issue `/opt/3par/vcdbaora/bin/vcdba_config`, and then skip to step 4.

3 If you are using the menu-driven application, from the backup host:

   a Select option **1**, **Configuration Administration**.

   b Select option **1**, **Create a backup Configuration**.

4 When prompted, press ENTER.

   - `Enter ORACLE_SID of the database instance [h=help,q=quit]?`

     Enter ORACLE_SID of the database instance that you want to configure. If the database is an RAC database, enter ORACLE_SID of any RAC instance.

   - `Enter hostname of the primary (database) server [h=help,q=quit]?`

     Enter the host name of the corresponding database server where the specified database instance is running.

   - `Select remote shell command [r=rsh,s=ssh,h=help,q=quit]?`

     This question is only for Solaris systems. SSH is the only connection method supported by Recovery Manager for Linux systems. Recovery Manager requires that either RSH (Solaris only) or SSH is configured to allow remote accesses between the backup host, the primary host, the InServ Storage Server, and Veritas NetBackup server.

     Enter `r` for RSH, or `s` for SSH.

   - `Enter ORACLE_HOME on the primary host [h=help,q=quit]?`

     Recovery Manager provides a default value for the ORACLE_HOME of the specified database instance if it can be retrieved from the `oratab` file.

     Press ENTER to accept default value or enter the ORACLE_HOME location of the specified database instance.

   - `Enter ORACLE_HOME on the backup host [h=help,s=skip,q=quit]?`

     Recovery Manager assumes that the ORACLE_HOME on the backup host is the same as the ORACLE_HOME on the primary host for the created clone database and RMAN backup. If you don’t intend to startup the clone database using the virtual copy on the backup host, you may skip it.

NOTE: RMAN backup requires the cloned database in mounted status. Therefore, ORACLE_HOME must be installed on the backup host.

Press ENTER to accept default value or enter the ORACLE_HOME location on the backup host.

- `Enter ORACLE_HOME of ASM instance on the primary server [h=help,q=quit]?`

  Recovery Manager provides a default value for the ORACLE_HOME of the ASM instance on the primary host if it can be retrieved from the `oratab` file.

  Press ENTER to accept the default value or enter ORACLE_HOME of the ASM instance on the primary host.

- `Enter ORACLE_HOME of ASM instance on the backup server [h=help,q=quit]?`

  Recovery Manager assumes that the ORACLE_HOME of the ASM instance on the backup host is the same as the ORACLE_HOME on the primary host.

  Press ENTER to accept the default value or enter ORACLE_HOME of the ASM instance on the backup host.

- `Enter Oracle parameter file of the database instance [h=help,q=quit]?`

  The Oracle parameter file can be either a `pfile` or an `spfile`. Recovery Manager recommends that an `spfile` is used, especially if the database is an RAC database.

  Recovery Manager provides a default value for the Oracle parameter file if it can be retrieved from the specified database itself.

  Press ENTER to accept default value, or enter a correct value for the Oracle parameter file.

- `Enter Oracle password file of the database instance [h=help,s=skip,q=quit]?`

  Recovery Manager provides a default value for the Oracle password file of the specified database instance. If the database does not have a password file, enter `s` or S to skip.

  Press ENTER to accept the default value or enter the Oracle password file of the specified database instance.

- `Do you want to setup configuration for remote copy? [y,n,q]? (n)`

  Select `n` if this configuration is not for 3PAR Remote Copy.

- `Enter InServ name [h=help,q=quit]?`

Enter the system name of the InServ Storage Server that is connected to both the primary and the backup hosts. The InServ Storage Server's name can be retrieved from the output of the `showsys` InForm CLI command.

- `Enter InServ hostname (from showhost output) of the backup server [h=help,q=quit]?`

  The hostname defined in the InServ Storage Server for the backup host can be retrieved from the output of the 3PAR InForm CLI `showhost` command on the InServ Storage Server.

  The InServ Storage Server's host name of the backup host may not be the same as the DNS host name of the backup host.

- `Enter InServ's user name for primary host [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected SSH as the remote shell.

  Recovery Manager requires that a 3PAR InForm user must have been created on the InServ Storage Server to allow access from the primary host to the InServ Storage Server.

- `Enter 3PAR password file on primary host [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected RSH as the remote shell.

  Recovery Manager requires that a 3PAR password file must have been created on the primary host to allow access to the 3PAR InForm CLI from the primary host.

- `Enter InServ's user name for the backup host [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected SSH as the remote shell.

  Recovery Manager requires that a 3PAR InForm user must have been created on the InServ Storage Server to allow access from the backup host to the InServ Storage Server.

- `Enter 3PAR password file on backup host [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected RSH as the remote shell.

  Recovery Manager requires that a 3PAR password file must have been created on the backup host to allow access to the 3PAR InForm CLI from the backup host.

- `Enter maximum number of virtual copies allowed [h=help,q=quit]?`

  Enter the maximum number of virtual copies that can be created for the specified database. Once the maximum number of virtual copies for the database is reached, Recovery Manager removes the oldest virtual copy before creating a new one.

  The default maximum number is 500 read-only virtual copies for each volume.

- `Select third-party backup tool [0=None,1=Veritas NBU,2=Oracle RMAN,h,q]?`

  Recovery Manager supports NBU (user-managed) backup and Oracle RMAN backup. Enter `0` if you do not want to perform backup.

  If you enter `0`, stop here. No further information is required. If you enter either `1` or `2`, you will be prompted for the following information:

- `Do you want to remove virtual copy after backup complete?  [y,n,q]?`

  Enter `n` if you do not want to remove the virtual copy after a backup is completed successfully. Otherwise, enter `y`.

- `Enter Oracle RMAN connection string [user/password@catdb,h,q]?`

  You will only be prompted with this question if you previously selected Oracle RMAN as the third-party backup tool.

  Enter the Recovery Catalog connection string in `user/passwd@catdb` format, where `catdb` is the service name of the Recovery Catalog, and `user/passwd` is the user name and password to be used to connect to the Recovery Catalog.

- `Enter Oracle RMAN channel type [d=DISK,s=SBT_TAPE,h,q]?`

  You will only be prompted with this question if you previously selected `Oracle RMAN` as the third-party backup tool.

  Enter `d` if you want to backup to local disk, or `s` if you want to backup to tape through Veritas NetBackup Media server.

- `Enter number of channels to be allocated [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected `Oracle RMAN` as the third-party backup tool.

  Enter the number of RMAN channels to be allocated for backup.

- `Enter NetBackup master server name [h=help,q=quit]?`

Enter the DNS host name of the Veritas Netbackup master server.

- `Enter NetBackup policy name for database backup [h=help,q=quit]?`

  Recovery Manager requires that an NBU backup policy must have been created for database backup.

- `Enter NetBackup full schedule name for database policy [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected `Veritas NBU` as the third-party backup tool.

  Enter a schedule name for the policy that is used to perform full database backup.

- `Enter NetBackup policy name for archivelog backup [h,q]?`

  A separate Veritas NetBackup policy must have been created for archive log back up if you want to perform back up of archive logs only. Enter the archive log backup policy, or press ENTER if you do not want to perform archive log back up.

- `Enter NetBackup full schedule name for archivelog policy [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected `Veritas NBU` as the third-party backup tool.

  Enter a schedule name of type full for the policy that is used to perform archive log backup.

- `Enter NetBackup incremental schedule name for archivelog policy [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected Veritas NBU as the third-party backup tool.

  Enter a schedule name of type differential/cumulative incremental for the policy that is used to perform archive log backup.

4.9.1.2 Creating a Recovery Manager Configuration File using the GUI on the Backup Host

To use the Recovery Manager GUI to create a Recovery Manager configuration file without Remote Copy support:

1 Start the Recovery Manager GUI on the backup host.

   a Ensure the X11 server is running on the destination host where the GUI is displayed. If the X11 server is not running, issue the following command:

```
<backup host># xhost +
```

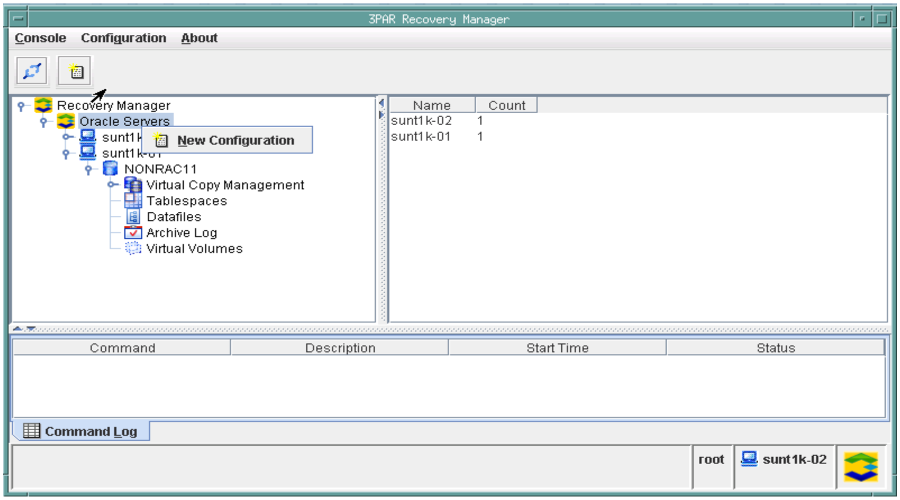
   b Ensure the DISPLAY environment variable is set.

```
<backup host># echo $DISPLAY
```

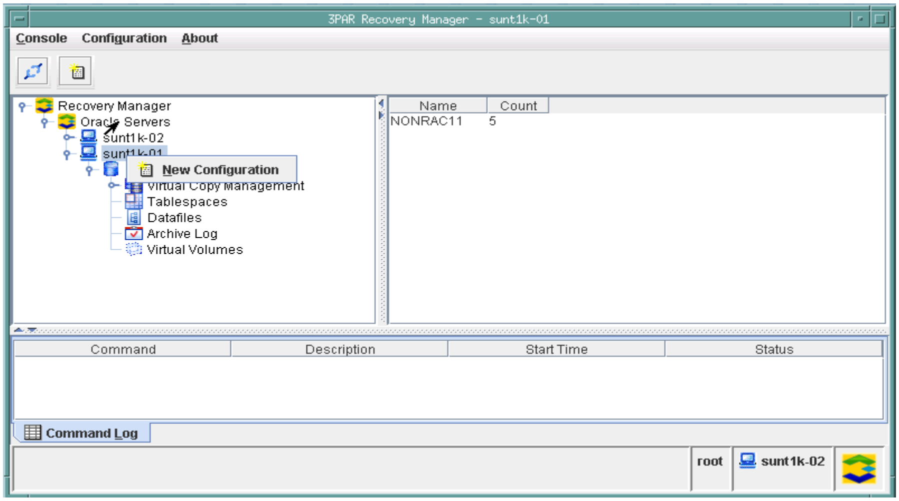
   c Start the Recovery Manager GUI.

```
<backup host># /opt/3par/vcdbaora/bin/vcdbagui
```

2 From the navigation window, right-click either the **Oracle Servers** node or a host node, and then select **New Configuration** as shown in the following figures.

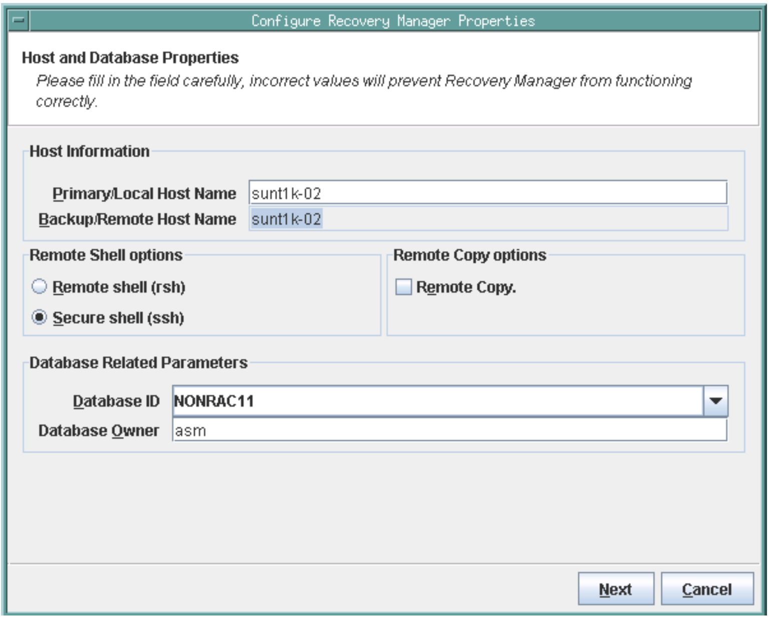


Name	Count
sunt1k-02	1
sunt1k-01	1



Name	Count
NONRAC11	5

The **Host and Database Properties** screens appear.



Host and Database Properties

Please fill in the field carefully, incorrect values will prevent Recovery Manager from functioning correctly.

Host Information

Primary/Local Host Name: sunt1k-02

Backup/Remote Host Name: sunt1k-02

Remote Shell options

○ Remote shell (rsh)

● Secure shell (ssh)

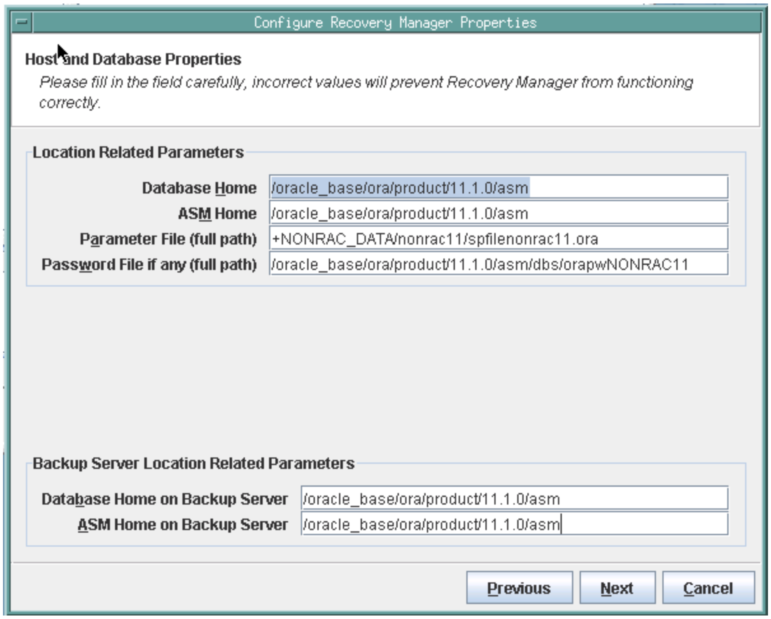
Remote Copy options

□ Remote Copy.

Database Related Parameters

Database ID: NONRAC11

Database Owner: asm



Host and Database Properties

Please fill in the field carefully, incorrect values will prevent Recovery Manager from functioning correctly.

Location Related Parameters

Database Home: /oracle_base/ora/product/11.1.0/asm

ASM Home: /oracle_base/ora/product/11.1.0/asm

Parameter File (full path): +NONRAC_DATA/nonrac11/spfilenonrac11.ora

Password File if any (full path): /oracle_base/ora/product/11.1.0/asm/dbs/orapwNONRAC11

Backup Server Location Related Parameters

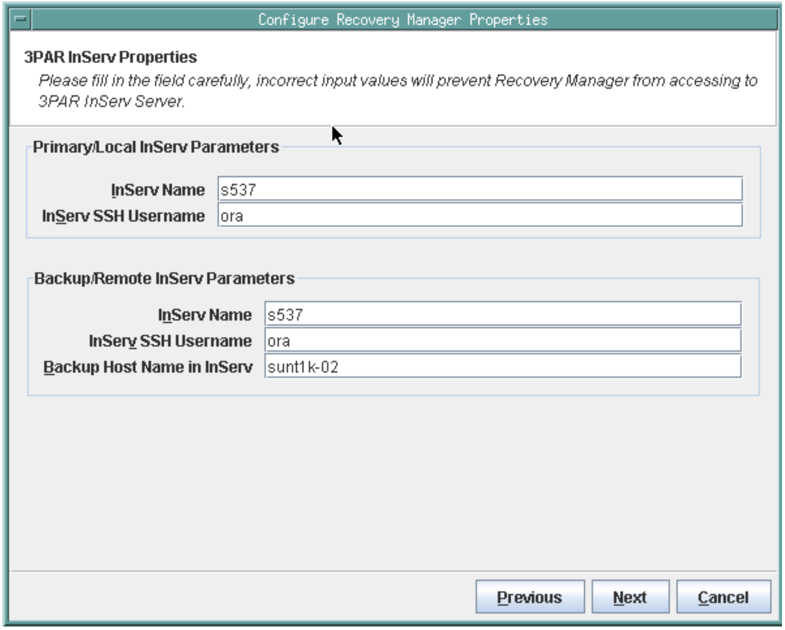
Database Home on Backup Server: /oracle_base/ora/product/11.1.0/asm

ASM Home on Backup Server: /oracle_base/ora/product/11.1.0/asm

3 Configure the host and database by entering the requested information on the configuration screen and click **Next**.

The **Modify Recovery Manager Configuration Properties** screen appears.

4 The **3PAR InServ Properties** screen appears.



3PAR InServ Properties

Please fill in the field carefully, incorrect input values will prevent Recovery Manager from accessing to 3PAR InServ Server.

Primary/Local InServ Parameters

InServ Name: s537

InServ SSH Username: ora

Backup/Remote InServ Parameters

InServ Name: s537

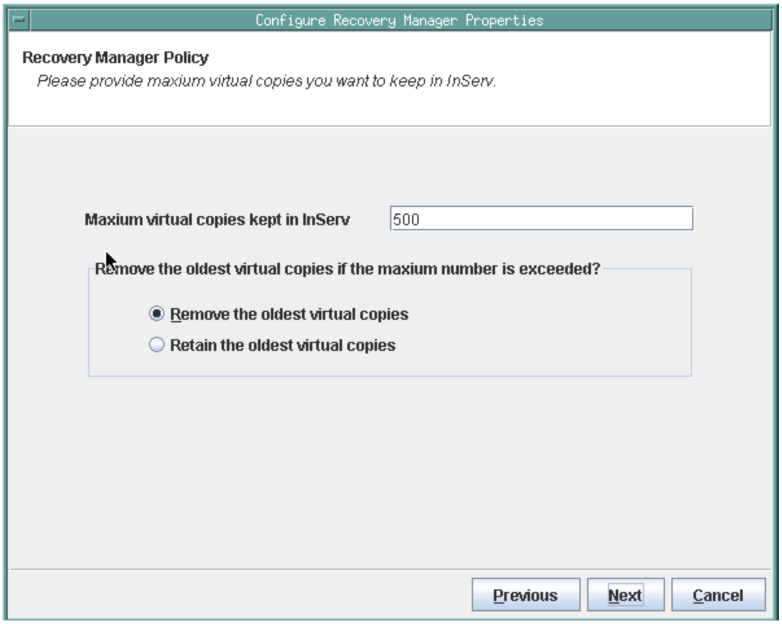
InServ SSH Username: ora

Backup Host Name in InServ: sunt1k-02

5 Depending on the connection option you choose, perform one of the following:

- (For Solaris systems) If you selected the **Remote Shell (RSH)** option when configuring the database, enter the requested information on the screen and click **Next**.
- If you selected the **Secure Shell (SSH)** option when configuring the database, enter the requested information on the configuration screen and click **Next**.

The **Recovery Manager Policy** screen appears.



Configure Recovery Manager Properties

Recovery Manager Policy

Please provide maxium virtual copies you want to keep in InServ.

Maxium virtual copies kept in InServ: 500

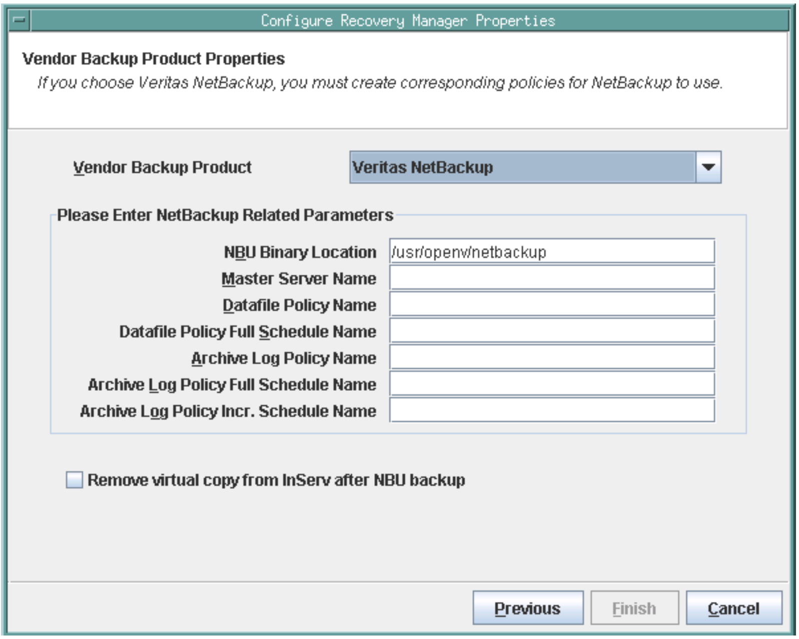
Remove the oldest virtual copies if the maxium number is exceeded?

● Remove the oldest virtual copies

○ Retain the oldest virtual copies

6 Specify the maximum number of virtual copies allowed in the InServ Storage Server. You can select to retain or remove the oldest virtual copy if the maximum number of virtual copies is reached. Click **Next**.

The **Vendor Backup Product Properties** screen appears.



Configure Recovery Manager Properties

Vendor Backup Product Properties

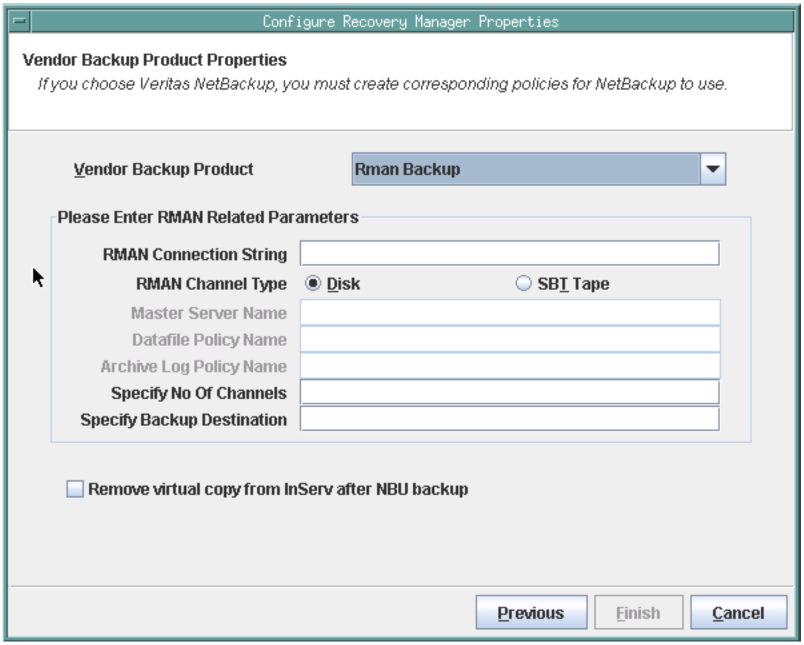
If you choose Veritas NetBackup, you must create corresponding policies for NetBackup to use.

Vendor Backup Product: Veritas NetBackup

Please Enter NetBackup Related Parameters

NBU Binary Location	/usr/openv/netbackup
Master Server Name	
Datafile Policy Name	
Datafile Policy Full Schedule Name	
Archive Log Policy Name	
Archive Log Policy Full Schedule Name	
Archive Log Policy Incr. Schedule Name	

□ Remove virtual copy from InServ after NBU backup



Configure Recovery Manager Properties

Vendor Backup Product Properties

If you choose Veritas NetBackup, you must create corresponding policies for NetBackup to use.

Vendor Backup Product: Rman Backup

Please Enter RMAN Related Parameters

RMAN Connection String	
RMAN Channel Type	● Disk ○ SBT Tape
Master Server Name	
Datafile Policy Name	
Archive Log Policy Name	
Specify No Of Channels	
Specify Backup Destination	

□ Remove virtual copy from InServ after NBU backup

7 Select the **Vendor Backup Product** from the menu.

8 Enter the requested information under **Related Parameters**.

- The NetBackup policies must be pre-created.
- One policy is used for backing up the entire database. This may or may not include an archive log destination, depending on the type of backup (online or offline), and requires one full schedule.
- The other policy is used only for backing up the main archive log destination. This requires both a full and differential schedule.
- If you do not want to delete the virtual copy after backing it up, deselect the **Remove virtual copy from InServ after NBU backup** option.

9 Click **Finish**.

Recovery Manager verifies the following:

- Connections between the backup host and the primary host.
- Connections between the backup host and the InServ Storage Server.
- Connections between the primary host and the InServ Storage Server.
- Connections between the backup host and the NetBackup master server (if NetBackup is selected).

If Recovery Manager successfully connects to the database, Recovery Manager retrieves the database tablespaces, datafiles, the archive log destination, and the virtual volumes where the database resides.

After verification is completed. Recovery Manager creates a virtual copy repository on the backup host (`/etc/3par/solutions/<primary_host>.ora.<oracle_sid>`) and two configuration files are generated along with one subdirectory for database files mapping information.

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config
```

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config_exp.sh
```

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/gui
```

4.9.2 Creating a Recovery Manager Configuration File Using Remote Copy

Before creating the configuration files for Recovery Manager to use, you must do the following:

- Set up physical links between the local and remote InServ systems. Refer to the *3PAR Remote Copy User’s Guide* for instructions on setting up links.
- Set up Remote Copy targets for the local and remote InServ systems.
- Create one Remote Copy groups, assign all virtual volumes used by datafiles and archive log destinations to the group.

> **CAUTION:** If Veritas Volume Manager is being used when assigning 3PAR virtual volumes to Remote Copy groups, all volumes in the same Veritas disk group should be assigned to one Remote Copy group, whether they are actually being used by the Oracle database or not. Otherwise, you might not be able to import and mount file systems on the remote backup host. Therefore, it is strongly suggested that Veritas disk groups only contain files used by one Oracle database.

- Start Remote Copy and verify its setup.

4.9.2.1 Creating Configuration Files using the Menu Driven Application or Command Line Interface on the Backup Host

To create the Recovery Manager configuration files:

1 From the backup host, start Recovery Manager.

```
<backup_host># /opt/3par/vcdbaora/bin/vcdba_main
```

2 If you are using the CLI, from the backup host, issue `/opt/3par/vcdbaora/bin/vcdba_config`, and then skip to step 4.

3 If you are using the menu-driven application, from the backup host:

a Select option **1, Configuration Administration**.

b Select option **1, Create A Backup Configuration**.

4 When prompted, press ENTER .

5 When prompted, answer the following questions:

- `Enter ORACLE_SID of the database instance [h,q]?`

  Enter ORACLE_SID of the database instance that you want to configure. If the database is an RAC database, enter ORACLE_SID of any RAC instance.

- `Enter hostname of the primary (database) server [h=help,q=quit]?`

  Enter the host name of the corresponding database server where the specified database instance is running.

- `Select remote shell command [r=rsh,s=ssh,h=help,q=quit]?`

  Recovery Manager requires that either RSH (Solaris only) or SSH is configured to allow remote accesses between the backup host, the primary host, the InServ Storage Server, and the Veritas NetBackup server.

  Enter `r` for RSH, or `s` for SSH.

- `Enter ORACLE_HOME on the primary host [h=help,q=quit]?`

  Recovery Manager provides a default value for the ORACLE_HOME of the specified database instance if it can be retrieved from the `oratab` file.

  Press ENTER to accept default value, or enter ORACLE_HOME location of the specified database instance.

- `Enter ORACLE_HOME on the backup host [h=help,q=quit]?`

  Recovery Manager assumes that the ORACLE_HOME on the backup host is the same as the ORACLE_HOME on the primary host

  Press ENTER to accept default value, or enter the ORACLE_HOME location on the backup host.

- `Enter ORACLE_HOME of ASM instance on the primary host [h=help,q=quit]?`

  Recovery Manager provides a default value for the ORACLE_HOME of the ASM instance on the primary host if it can be retrieved from the `oratab` file.

  Press ENTER to accept the default value, or enter the ORACLE_HOME of the ASM instance on the primary host.

- `Enter ORACLE_HOME of ASM instance on the backup host [h,q]?`

  Recovery Manager assumes that the ORACLE_HOME of the ASM instance on the backup host is the same as the ORACLE_HOME of the ASM instance on the primary host.

Press `enter` to accept the default value, or enter ORACLE_HOME of the ASM instance on the backup host.

- `Enter Oracle parameter file of the database instance [h,q]?`

  Oracle parameter file can be either a `pfile` or a `spfile`. Recovery Manager recommends that `spfile` is used, especially if the database is an RAC database.

  Recovery Manager provides a default value for the Oracle parameter file if it can be retrieved from the specified database itself.

  Press ENTER to accept default value or enter a correct value for the Oracle parameter file.

- `Enter Oracle password file of the database instance [h=help,s=skip,q=quit]?`

  Recovery Manager provides a default value for the Oracle password file of the specified database instance.

  Press ENTER to accept the default value or enter the Oracle password file of the specified database instance. If no password is being used, press 's' to skip it.

- `Do you want to setup configuration for remote copy? [y,n,q]? (y)`

  Select `y` if this is this configuration is for Remote Copy.

- `Enter Primary/Local InServ name [h=help,q=quit]?`

  Enter the system name of the primary/local InServ Storage Server that is connected to the primary host. The InServ Storage Server name can be retrieved from the output of InForm CLI `showsys` command.

- `Enter remote copy target name on primary/local InServ [h=help,q=quit]?`

  Enter the Remote Copy target name defined on the primary/local InServ Storage Server.

- `Enter remote copy group name for datafiles on primary/local InServ [h=help,q=quit]?`

  Recovery Manager requires that one Remote Copy group must have been created on the primary/local InServ Storage Server. The Remote Copy group must contain all virtual volumes used by the data files.

- `Enter remote copy group name for archive log on primary/local InServ [h=help,q=quit]?`

This question is for backwards compatibility. Provide the Remote Copy group name for the archive log destinations if it is being used. Press ‘s’ to skip it if there is no such group.

- `Enter Secondary/Remote InServ name [h=help,q=quit]?`

  Enter the system name of the Secondary/Remote InServ Storage Server that is connected to the backup host. The InServ Storage Server name can be retrieved from the output of the InForm CLI `showsys` command.

- `Enter remote copy target name on remote/secondary InServ [h=help,q=quit]`

  Enter the Remote Copy target name defined on the secondary/remote InServ Storage Server.

- `Enter InServ hostname (from showhost output) of the backup host [h=help,q=quit]?`

  The InServ Storage Server’s hostname of the backup host can be retrieved from the output of the InForm CLI `showhost` command on the secondary/remote InServ Storage Server.

  The InServ Storage Server’s hostname of the backup host may not be the same as the DNS hostname of the backup host.

  Press ENTER to accept the default value, otherwise, provide the correct hostname defined in the InServ Storage Server.

- `Enter Primary/Local InServ's user name [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected SSH as the remote shell.

  Recovery Manager requires that a 3PAR InForm user must have been created on the primary/local InServ Storage Server to allow access from the primary host to the primary/local InServ Storage Server.

- `Enter 3PAR password file on primary host [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected RSH as the remote shell.

  Recovery Manager requires that a 3PAR password file must have been created on the primary host to allow access to the Primary/Local InServ Storage Server from the primary host.

- `Enter Secondary/Remote InServ's user name [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected SSH as the remote shell.

  Recovery Manager requires that a 3PAR InForm user must have been created on the Secondary/Remote InServ Storage Server to allow access from the backup host.

- `Enter 3PAR password file on backup host [h=help,q=quit]?`

  You will only be prompted with this question if you previously selected RSH as the remote shell.

  Recovery Manager requires that a 3PAR password file must have been created on the backup host to allow access to the Secondary/Remote InServ Storage Server from the backup host.

4.9.2.2 Creating a Recovery Manager Configuration File using the GUI on the Backup Host

To use the Recovery Manager GUI to create a Recovery Manager configuration file with Remote Copy support, perform the following:

1 Start the Recovery Manager GUI on the backup host.

  a Ensure the X11 server is running on the destination host where the GUI is displayed. If the X11 server is not running, enter the following command:

```
<backup_host># xhost +
```

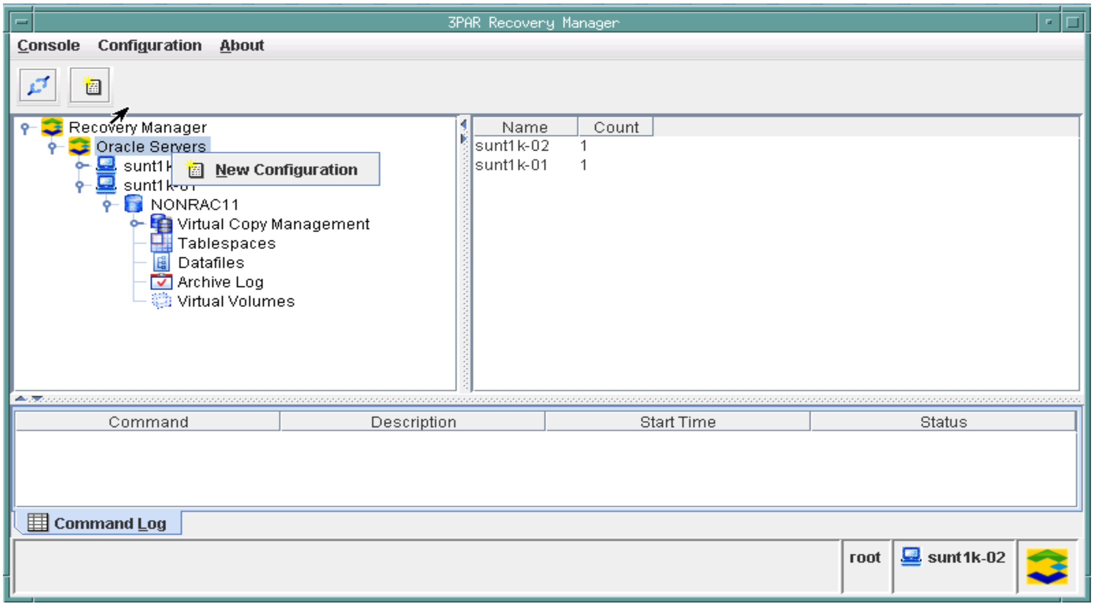
  b Ensure the DISPLAY environment variable is set.

```
<backup_host># echo $DISPLAY
```

  c Start the Recovery Manager GUI.

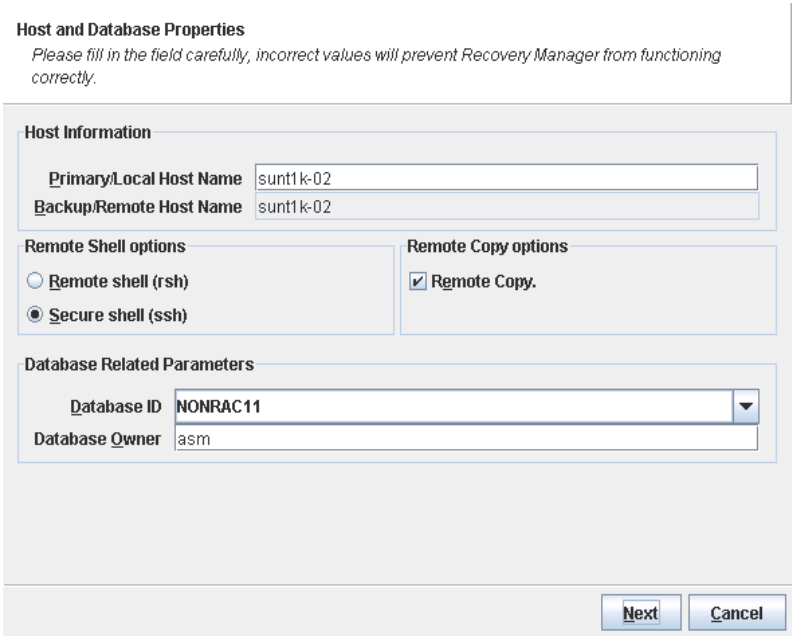
```
<backup_host># /opt/3par/vcdbaora/bin/vcdbagui
```

2 From the navigation window, right-click either the **Oracle Servers** node or the host node, and then select **New Configuration** as shown in the following figures.



Name	Count
sunt1k-02	1
sunt1k-01	1

The **Host and Database Properties** screen appears.



Host and Database Properties

Please fill in the field carefully, incorrect values will prevent Recovery Manager from functioning correctly.

Host Information

Primary/Local Host Name	sunt1k-02
Backup/Remote Host Name	sunt1k-02

Remote Shell options

○ Remote shell (rsh)

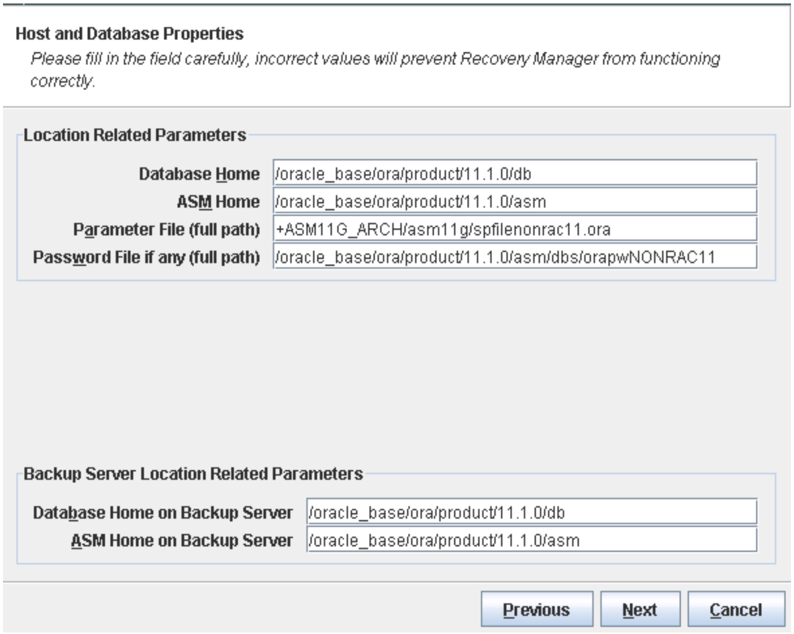
● Secure shell (ssh)

Remote Copy options

☑ Remote Copy.

Database Related Parameters

Database ID	NONRAC11
Database Owner	asm



Host and Database Properties

Please fill in the field carefully, incorrect values will prevent Recovery Manager from functioning correctly.

Location Related Parameters

Database Home: /oracle_base/ora/product/11.1.0/db

ASM Home: /oracle_base/ora/product/11.1.0/asm

Parameter File (full path): +ASM11G_ARCH/asm11g/spfilenonrac11.ora

Password File if any (full path): /oracle_base/ora/product/11.1.0/asm/dbs/orapwNONRAC11

Backup Server Location Related Parameters

Database Home on Backup Server: /oracle_base/ora/product/11.1.0/db

ASM Home on Backup Server: /oracle_base/ora/product/11.1.0/asm

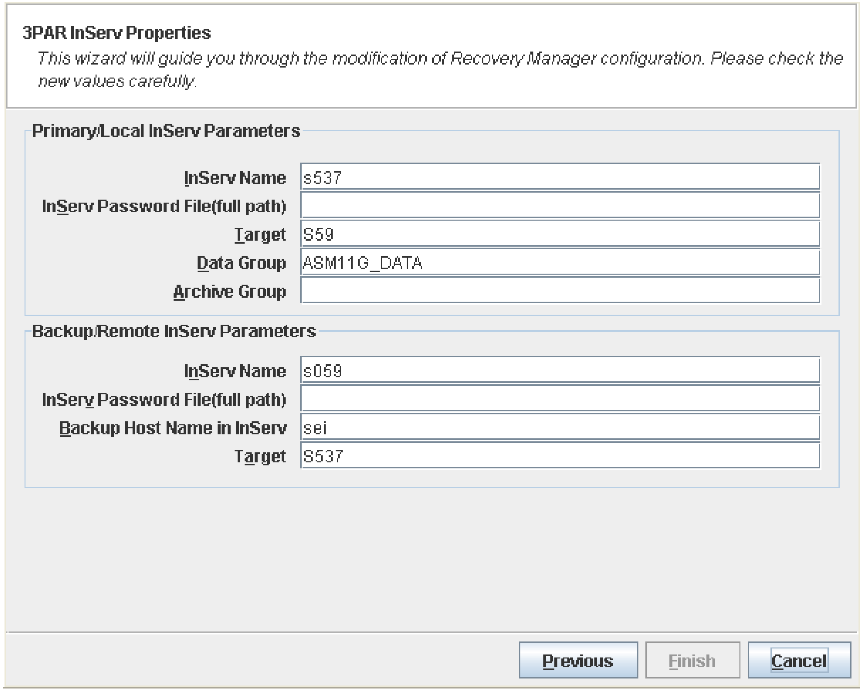
3 Configure the host information and database related parameters by entering the requested information on the **Host and Database Properties** screen.

   a Check the **Remote Copy** option.

   b Click **Next**.

4 Depending on the connection type you chose in step 3 on page 4.46, provide the following information in the **3PAR InServ Properties** screen that appears:

- For RSH connection (Solaris systems only), enter the following information and then click **Finish.**



3PAR InServ Properties

This wizard will guide you through the modification of Recovery Manager configuration. Please check the new values carefully.

Primary/Local InServ Parameters

InServ Name	s537
InServ Password File(full path)	
Target	S59
Data Group	ASM11G_DATA
Archive Group	

Backup/Remote InServ Parameters

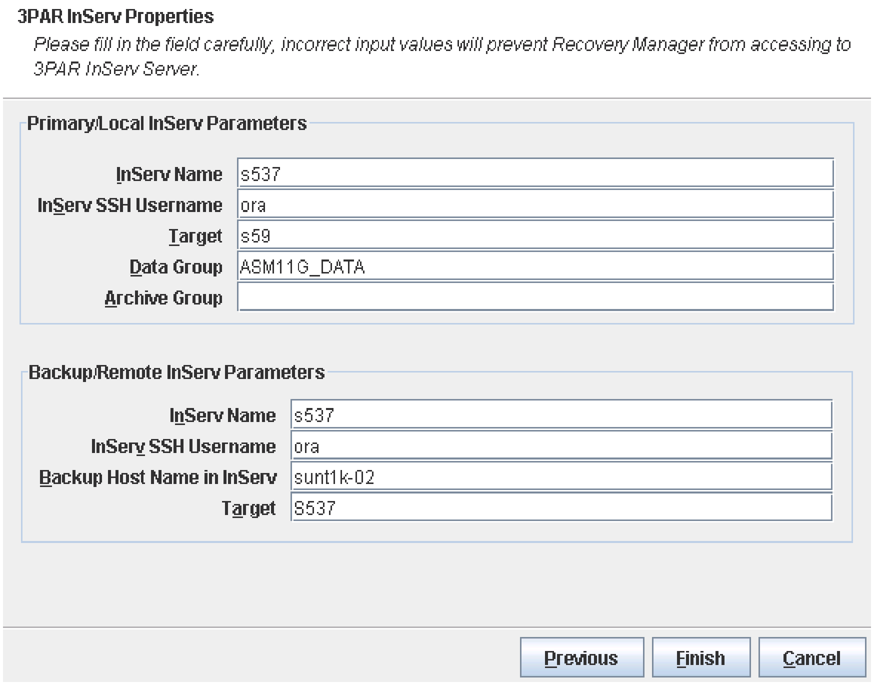
InServ Name	s059
InServ Password File(full path)	
Backup Host Name in InServ	sei
Target	S537

In the example above:

- **InServ Name**: name of the primary/local or secondary/remote InServ Storage Server.
- **InServ Password File**: location of the storage server client password file.
- **Target**: the name of the target InServ Storage Server. On the primary/local and secondary/remote systems, use the InForm CLI `showrcopy targets` command to display the defined target names
- **Data Group**: the Remote Copy group name for the virtual volumes where the datafiles are located. In a single Remote Copy configuration, datafiles and archive log destinations virtual volumes are included in the same Remote Copy group.
- **Archive Group**: the Remote Copy group name of the virtual volumes where the database archive logs are located. In a single Remote Copy configuration, datafiles and archive log destinations virtual volumes are included in the same Remote Copy group. This parameter can be left empty.

- **Backup Host Name in InServ**: the backup host hostname defined in the InServ Storage Server. Use the InForm CLI `showhost` command to see a list of defined hosts.

- For SSH connection, enter the requested information on the configuration screen and click **Finish**.



3PAR InServ Properties

Please fill in the field carefully, incorrect input values will prevent Recovery Manager from accessing to 3PAR InServ Server.

Primary/Local InServ Parameters

InServ Name: s537
InServ SSH Username: ora
Target: s59
Data Group: ASM11G_DATA
Archive Group:

Backup/Remote InServ Parameters

InServ Name: s537
InServ SSH Username: ora
Backup Host Name in InServ: sunt1k-02
Target: S537

In the example above:

- **InServ Name**: name of the primary/local or secondary/remote InServ Storage Server.

- **InServ SSH username**: InServ Storage Server username (login).

- **Target**: the name of the target InServ Storage Server. On the primary/local and secondary/remote systems, use the InForm CLI `showrcopy targets` command to display the defined target names.

- **Data Group**: the Remote Copy group name for the virtual volumes where the datafiles are located. In a single Remote Copy configuration, datafiles and archive log destinations virtual volumes are included in the same Remote Copy group.

  - **Archive Group**: the Remote Copy group name of the virtual volumes where the database archive logs are located. In a single Remote Copy configuration, datafiles and archive log destinations virtual volumes are included in the same Remote Copy group.
  - **Backup Host Name in InServ**: the backup host hostname defined in the InServ storage system. Use the InForm CLI `showhost` command to see a list of defined hosts.

The **Verification** screen appears.

Recovery Manager verifies the following:

- Connections between the backup host and the primary host.
- Connections between the backup host and the InServ Storage Server.
- Connections between the primary host and the InServ Storage Server.
- Database ID.
- Remote Copy configuration.

After the verification is complete, Recovery Manager creates a virtual copy repository on the backup host (`/etc/3par/solutions/<primary_host>.ora.<oracle_sid>`) and two configuration files are generated along with one subdirectory for the database files mapping information.

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config
```

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config_exp.sh
```

```
/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/gui
```

5
Using Recovery Manager from the Menu-Driven Application

In this chapter

Read this chapter for instructions on using Recovery Manager for Oracle from the menu-driven application.

5.1 Starting the Menu-Driven Application

NOTE: New features will no longer be added into menu-driven applications.

To start the Recovery Manager menu-driven application:

```
<backup_host># /opt/3par/vcdbaora/bin/vcdba_main
```

NOTE: Refer to *4.9.1.1 Creating Configuration Files using the Menu-Driven Application or the Command Line Interface on the Backup Host* on page 4.27 for instructions on creating a configuration file using the menu-driven application.

5.2 Managing Virtual Copies

Recovery Manager for Oracle provides tools to manage the virtual copies. The tools allow for creating, displaying, removing, mounting and unmounting virtual copies.

To manage virtual copies from the menu-driven application:

1. On the **3PAR Recovery Manager for Oracle** main menu, select option **2**, **Virtual Copy Management**.
2. Select a primary host and database configuration with which you wish to work.

   The **Virtual Copy Management** menu screen appears.

5.2.1 Displaying Virtual Copies

To display virtual copies:

1. On the **Virtual Copy Management** menu screen, select option **1**, **Display Virtual Copy**.
2. Select the virtual copy to display.

   Possible values for the virtual copy type are:

   - `Online` - virtual copy is created while the database is up and running, the virtual copy contains datafiles and archive log files; it is a hot backup.
   - `Offline` - virtual copy is created while the database is down. It is a cold backup.
   - `Datafile` - virtual copy is created for data files only while the database is open.
   - `Archlog` - virtual copy is created for archive log destination only.

   Possible values for the virtual copy status are:

   - `Available` - the virtual copy is available to be used.
   - `Removed` - the virtual copy has been removed from the InServ Storage Server.
   - `Mounted` - the virtual copy has been mounted on the backup host.
   - `Database` - the virtual copy is currently used for the cloned database on the backup host. The cloned database is up and running.
   - `Mounted(P)` - the virtual copy has been partially mounted, there are some errors while mounting the virtual copy. You need to either unmount it and remount it, or call 3PAR support.

   Possible values for the virtual copy backup status are:

   - `N` - The virtual copy has not been backed up.
   - `Y (Full)` - The virtual copy has been backed up as a full backup.
   - `Y (Incr)` - The virtual copy has been backed up as a differential incremental backup.
   - `Y (Cinc)` - The virtual copy has been backed up as a cumulative incremental backup.

5.2.2 Creating a Virtual Copy

NOTE: If Recovery Manager is configured to use RMAN backup, a Recovery Catalog must have been created and configured prior to creating the virtual copy.

To create a virtual copy:

1. On the **Virtual Copy Management** menu screen, select menu option **2**, **Create Virtual Copy**.
2. When prompted, choose to create a virtual copy for the database (d) or `archive log destination only(a)`.
3. If you choose to create a virtual copy for the database, enter `o` (online) or `f` (offline) to create an online or offline virtual copy.

NOTE: If a virtual copy is created offline, the database must be shut down prior to creating the virtual copy. If you try to create an offline virtual copy with the database running, you will get an error.

5.2.3 Removing a Virtual Copy

To remove a virtual copy:

1. On the **Virtual Copy Management** menu screen, select option **3**, **Remove Virtual Copy**.
2. On the **Remove Virtual Copy** menu, select the virtual copy to remove.
   - The virtual copy removal utility only removes the actual virtual copy. It does not remove the repository information for restoration purpose, in the case that the virtual copy is not backed up, the repository will be removed as well.
   - If the repository still remains and the virtual copy is backed up to media before being removed, you can still restore to that point-in-time virtual copy from the backup image.
   - The status of the virtual copy shows Removed after the virtual copy is removed.

5.2.4 Mounting a Virtual Copy

To mount a virtual copy:

1. On the **Virtual Copy Management** menu screen, select option **4**, **Mount Virtual Copy**.
2. Select the virtual copy to be mounted.
   - Recovery Manager creates a read/write virtual copy from the read-only (original) virtual copy and then mounts the read-write virtual copy. Any changes to the read-write virtual copy will not affect the read-only virtual copy.
   - The virtual copy is mounted at a default mount point, unless an alternate mount point is specified.
   - See section *2.6.4 The Virtual Copy Mount Utility* on page 2.10 for instructions on mounting ASM-based databases.

5.2.5 Unmounting a Virtual Copy

To unmount a virtual copy:

1. On the **Virtual Copy Management** menu screen, select option **5**, **Unmount Virtual Copy**.
2. Select the virtual copy to unmount.

   During unmounting, Recovery Manager removes the read/write virtual copy, as well as any directories that were created during the **Mount Virtual Copy** operation.

   See section *2.6.5 The Virtual Copy Unmount Utility* on page 2.11 for instructions on unmounting ASM-based databases.

5.2.6 Exporting a Virtual Copy

To export a virtual copy:

1. On the **Virtual Copy Management** menu screen, select option **6**, **Export Virtual Copy**.
2. Select the virtual copy to be exported.
3. When prompted, answer the following questions:
   a. **Do you want to export Virtual Copy** `<name> [y,n,q]`

Answer y (yes).

b **Enter alternate backup host**

Provide the name of the host where the virtual copy is exported.

c **Enter InServ internal host name for alternate backup host?**

Provide the 3PAR InServ Storage Server internal host name that represents the backup host on the InServ Storage Server (the `showhost` command displays the list of hosts defined on the storage server).

d **Enter full path of 3PAR InServ password file...**

1) Provide the 3PAR password file location for the alternate backup host if the current connection method between backup host and the server is using RSH.

2) Provide the InServ Storage Server's user name if the current connection method between backup host and the InServ Storage Server is using the SSH method.

5.2.7 Removing a Virtual Copy's Repository

To remove a virtual copy repository:

1. On the **Virtual Copy Management** menu screen, select option **7**, **Remove Virtual Copy Repository**.
2. Select the virtual copy repository to remove.

NOTE: Only a virtual copy that has Removed status can be specified.

5.2.8 Setting Virtual Copy Policy

To set the virtual copy policy:

1. On the **Virtual Copy Management** menu screen, select option **8**, **Virtual Copy Policy**.
2. When prompted, enter the maximum number of virtual copies to be maintained at any time. The maximum allowed virtual copy number is 500.
3. The application now asks you if you want to remove the oldest virtual copy when the maximum number of virtual copies is reached. Enter y or n.

4. Finally, you are asked if you want to save this new policy. Enter y, n, or q.

> **NOTE:** If you do not wish to remove the oldest virtual copy while creating the new virtual copy, and the InServ Storage Server contains the maximum number of virtual copies allowed, the next virtual copy creation will fail.

5.3 Backing Up Virtual Copies

> **NOTE:** Backup is not supported on Remote Copy configuration.

Read the following sections for information about backing up virtual copies using Recovery Manager.

5.3.1 Performing Immediate Backups

To perform immediate backups using the menu-driven application:

1. On the **3PAR Recovery Manager for Oracle** main menu, select option **3**, **Backup Administration**.
2. Select the database to be backed up.
3. When prompted to backup the existing virtual copy, enter y, n, or q?

   If you answer `n` to backup the existing virtual copy, the program creates the new virtual copy, and the next screen to appear allows you to select either `Backup Database` or `Backup Archive Log Destination`.

```
 3PAR Recovery Manager for Oracle

Backup Administration: Perfom backup operation from backup host

 1. Backup Database
 2. Backup Archive Log Destination

 ?. Help For Current Menu
 r. Return To The Previous Menu
 x. Exit From Utility

 Enter Selection ->
```

- `Backup Database`

  Select this option to perform database backup. You are asked to confirm for a configuration file, which you should have already created (see *4.9 Recovery Manager Configuration Files* on page 4.27).

- `Backup Archive Logs Destination`

  Select this option to create a virtual copy of the archive log destination only. You are asked for a configuration file, which you should have already created (see *4.9 Recovery Manager Configuration Files* on page 4.27).

5.3.2 Performing Automatic Backups

If you have created a NetBackup policy and a configuration file for a database instance, NetBackup triggers a backup automatically.

NOTE: When you configure a NetBackup policy, to trigger automatic backups, you must specify a backup window for each schedule in each policy.

NOTE: If an Egenera server is used as a backup host, Recovery Manager does not support automatic backup.

5.4 Performing Restores

You can automatically restore a backup of a database instance only if the backup was created using NetBackup.

The backup operation actually occurs on the backup host. Restoring a backup image from the backup host to the primary host is called *alternate restore*. NetBackup requires that a file name of `/usr/openv/netbackup/db/altnames/<database_hostname>` exist on the NetBackup master server.

For example, if you want to restore a backup image to a database server named `pilot`, create an empty file named `pilot` in `/usr/openv/netbackup/db/altnames` on the NetBackup master server.

5.4.1 Performing Restores

NOTE: Restore is not supported on Remote Copy configuration.

To perform a restore using the menu-driven application:

1. On the **3PAR Recovery Manager for Oracle** main menu, select option **4**, **Restore Administration**.
2. Select a database to restore.
3. 3PAR Virtual Copy then displays a list of virtual copies. Each virtual copy is represented by virtual copy timestamp, actual backup timestamp, backup type, status and a flag to backup to media. Choose a virtual copy to restore the database from its associated backup image.
4. Choose whether to restore the backup image that is associated with the selected virtual copy to its original location, or to a common mount point on the primary or backup host.

5.5 Performing Periodic Remote Copy

To perform periodic Remote Copy from the menu-driven application:

1. On the **3PAR Recovery Manager for Oracle** main menu, select option **5**, **Remote Copy Administration**.
2. Select menu option **1**, **Periodic Synchronization**.
3. Select a database to begin synchronization.
4. When prompted, select `o` (online) or `f` (offline).

   The periodic synchronization is started. You cannot start a new periodic synchronization until the current one finishes.

   If you attempt another synchronization before the current operation completes, Recovery Manager returns an error. Issue the `showrcopy` command either from the primary/local InServ Storage Server, or from the secondary/remote InServ Storage Server to check the synchronization status (see the *InForm OS Command Line Interface Reference* for more information about the `showrcopy` command).

   Synchronization completion time varies depending on data changes, IO, and network traffic.

6 Using the Recovery Manager Command Line Interface

In this chapter

This chapter describes the Recovery Manager command line utilities.

NOTE: The command line utilities are located in `/opt/3par/vcdbaora/bin`.

Listed below are commands that can be run from the command line.

COMMAND

vcdba_backup

SYNTAX

```
vcdba_backup -s <oracle_sid> -p <primary_host> [-t <timestamp>]
[-o full|incr|cinc] [-v]
```

or

```
vcdba_backup -s <oracle_sid> -p <primary_host>
[-o online|offline|datafile|archonly [,full|incr|cinc] [-v]
```

DESCRIPTION

Recovery Manager integrates 3PAR Virtual Copy feature with Veritas NetBackup(NBU) and Oracle RMAN to perform off-host backup. Off-host backup can dramatically reduce performance impact on the database (primary) host as well as minimize database down time or the time database in backup mode during backup.

The first form of vcdba_backup command initiates an immediate backup of an existing database virtual copy. The virtual copy must have Available status (not mounted) in order to be backed up. The vcdba_backup command mounts the virtual copy to the backup host before initiating an immediate backup (off-host).

The second form of vcdba_backup command creates a new database virtual copy, mounts it to the backup host before initiating an immediate backup (off-host).

Recovery Manager supports NBU (user-managed) backup and Oracle RMAN back-up methods, which can be specified during the Recovery Manager configuration process. For the Oracle RMAN backup method, you can select the SBT_TAPE or DISK option to backup to tape or disk, respectively. Regardless of backup method, Recovery Manager supports full backup of an Oracle database or archive log destination. However, incremental (differential or cumulative) backup of the whole Oracle database is only available for Oracle RMAN backup method. Incremental (differential or cumulative) backup of archive log destination is only available for NBU (User-managed) backup method.

Backup is not supported on Remote Copy configuration.

The following are restrictions and automated scripts that are generated when configuring Recovery Manager. The automated scripts will be executed while the vcdba_backup command is running.

For NBU (user-managed) backup:

- The Veritas NetBackup client must be installed on the backup host and primary host.
- At least one NBU policy of standard type must be created and configured for database backup. Optionally, a separate NBU policy of standard type can be created and configured for archive log backup.
- When vcdba_backup is executed, it generates an include list file, that contains a list of datafiles and/or archive log destination on the mounted virtual copy and stores it in /usr/openv/netbackup/include_list.<policy_name> on the NBU client (the backup host).

For Oracle RMAN backup (to tape or disk):

- To perform RMAN backup to tape, the Veritas NetBackup client must be installed on the backup host and primary host. In addition, Veritas Netbackup for Oracle (Oracle Agent) must be installed on the backup host, primary host, and the NBU master server.
- To perform RMAN backup to tape, at least one NBU policy of Oracle type must be created and configured for database backup. Optionally, a separate NBU policy of Oracle type can be created and configured for archive log backup.
- Regardless of tape or disk backup, an Oracle RMAN Recovery Catalog database must be created and configured prior to running this command.
- During a backup, vcdba_backup starts up a clone database in MOUNTED mode using the mounted virtual copy on the backup host.
- During a backup, vcdba_backup executes the RMAN backup script vcdba_rman_dbbackup.sh or vcdba_rman_archbackup.sh to backup the clone data base.
- The RMAN backup scripts (vcdba_rman_dbbackup.sh and vcdba_rman_archbackup.sh) are generated at /etc/3par/solutions/<primary_host>.ora.<oracle_sid> during the creation of the Recovery Manager configuration file (see vcdba_config).

Depending on which backup method has been configured for the Recovery Manager, the vcdba_backup command performs the following actions:

- Creates a virtual copy (online, offline, or datafile) for the database or archive log destination if a virtual copy is not specified.
- Mounts the virtual copy on the backup host.

- For NBU (user-managed) backups, generates an include list file, that contains a list of datafiles and/or archive log destination on the mounted virtual copy and stores it in `/usr/openv/netbackup/include_list.<policy_name>` on the NBU client (the backup host).

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on the backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance ID of the primary database. For Real Application Cluster (RAC) databases, any instance ID can be specified.
- `-p <primary_host>` - The host name of the primary host, on which the Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy to be backed up. The virtual copy name can be obtained using the `vcdba_display` command.
- `-o online` - Creates an online virtual copy of a database while it is OPEN (online) prior to backup. This option is ignored if a virtual copy is specified. The `offline`, `online`, `datafile`, and `archonly` options are mutually exclusive.
- `-o hotbkup` - This option is the same as the `-o online` option. This option is deprecated and will be removed at a later release.
- `-o offline` - Creates an offline virtual copy of a database while it is CLOSED (offline) prior to backup. This option is ignored if a virtual copy is specified. The `offline`, `online`, `datafile`, and `archonly` options are mutually exclusive.
- `-o coldbkup` - Same as the `-o offline` option. This option is deprecated and will be removed at a later release.

- `-o datafile` - Creates an virtual copy for all datafiles (not including the archive log destinations) of a database while it is OPEN (online) prior to backup. This option is ignored if a virtual copy is specified. The `online`, `offline`, `datafile`, and `archonly` options are mutually exclusive. A virtual copy created with the `-o datafile` option is only useful when archive logfiles generated during the creation of the virtual copy are also available. You may want to create separate virtual copies using the `-o archonly` options, or use another backup method to backup archive log destinations.

- `-o archonly` - Creates a virtual copy of the archive log destination prior to backup. This option cannot be used if a virtual copy is specified. The `offline`, `online`, `datafile`, and `archonly` options are mutually exclusive.

- `-o full`- Performs a full backup of a virtual copy. If Veritas NetBackup is selected as the backup method, this option can be used with the `-o archonly` option to perform full backup of an archonly virtual copy. If Oracle RMAN is selected as the backup method, this option can be used to perform full backup of an online or offline virtual copy.

- `-o incr` - Performs an incremental backup of a virtual copy. If Veritas Netbackup is selected as the backup method, this option can be used with the `-o archonly` option to perform incremental backup of an archonly virtual copy. If Oracle RMAN is selected as the backup method, this option can be used to perform an incremental backup of an online or offline virtual copy.

- `-o cinc` - Performs a cumulative incremental backup of a virtual copy. If Veritas NetBackup is selected as the backup method, this option can be used with the `-o archonly` option to perform a cumulative incremental backup of an archonly virtual copy. If Oracle RMAN is selected as the backup method, this option can be used to perform a cumulative incremental backup of an online or offline virtual copy.

- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

vcdba_checkconfig

SYNOPSIS

```
vcdba_checkconfig [-s <oracle_sid> -p <primary_host>]
[-o all|skipdatabase|databaseonly] [-v]
```

DESCRIPTION

The vcdba_checkconfig command validates a Recovery Manager configuration file for a specified database. A configuration file must have been created prior to using this command.

By default, all configured parameters in the specified configuration file will be validated. One can select to validate only database parameters or non-database parameters.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on the backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- -s <oracle_sid> - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- -p <primary_host> - The corresponding hostname of the primary (database) host where the specified Oracle database instance is running. The value of the primary host name must match the output of the hostname command.
- -o all - Validates all parameters specified in the Recovery Manager configuration file.
- -o skipdatabase - Validates all non-database parameters specified in the Recovery Manager Configuration file.
- -o databaseonly - Validates all database parameters specified in the Recovery Manager Configuration file.
- -v - Runs the command in verbose mode to display useful messages.

COMMAND

```
vcdba_config
```

SYNOPSIS

```
vcdba_config [-s <oracle_sid> -p <primary_host>]
```

DESCRIPTION

The `vcdba_config` command creates or modifies the 3PAR Recovery Manager configuration file for a database. A configuration file for each database must be created prior to using any database snapshot (virtual copy) utilities provided by 3PAR Recovery Manager. The configuration file will be created at `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/config`.

An equivalent environment file is also automatically created for each created configuration file. It contains all configuration parameters specified in the configuration file. 3PAR Recovery Manager uses the environment file instead. The environment file is also stored at the same location as the configuration file.

`vcdba_config` is an interactive command. The command will prompt for necessary information depending on a user's selection. Generally, the command will prompt for the following information:

- `ORACLE_SID` - The Oracle database instance ID. For an RAC database, ORACLE_SID can be an SID of any instance.
- `ORACLE_HOME` - The location of Oracle Home on the database server of the specified database instance.
- `ORACLE_HOME_BACKUP` - The location of Oracle Home on the backup host.
- `ASM_ORACLE_HOME` - The location of Oracle Home of the ASM instance on the primary host. This parameter is only required if the specified database is using ASM.
- `ASM_ORACLE_HOME_BACKUP` - The location of Oracle Home of the ASM instance on the backup host. This parameter is only required if the specified database is using ASM.
- `ORACLE_OWNER` - Oracle database owner of the specified database instance.
- `ORACLE_INIT` - The Oracle database parameter file (`pfile`) or server parameter file (`spfile`) of the specified database instance. 3PAR Recovery Manager recommends that `spfile` should be used. For an RAC database, an `spfile` is required.
- `ORACLE_PWDFILE` - The Oracle password file of the specified database instance, if any.

- PRIMARYHOST - The hostname of the primary (database) server where the Oracle database instance is running. The value of the primary host name must match the output of the hostname command.
- TPDHOST - The backup hostname defined in the InServ Storage Server. The hostname can be obtained from the output of the showhost InForm CLI command, and may not be the UNIX hostname of the backup host.
- REMOTE_SHELL - The remote shell (SSH or RSH) to be used by 3PAR Recovery Manager to remotely execute commands on the primary host, backup host, or InServ Storage Server. The remote shell must be configured on the primary host, backup host, and InServ Storage Server prior to running the vcdba_config command.
- TPDSYSNAME_PRIMARY - The 3PAR InServ Storage Server node name, which is connected to the primary host
- TPDSYSNAME_BACKUP - The 3PAR InServ Storage Server node name, which is connected to the backup host.
- TPDUSERNAME_PRIMARY - The 3PAR InServ Storage Server CLI user name to be used to connect to the InServ Storage Server node from the primary host. This parameter is required if SSH is specified as remote shell.
- TPDUSERNAME_BACKUP - 3PAR InServ Storage Server CLI user name to be used to connect to the InServ Storage Server node from the backup host. This parameter is required if SSH is specified as remote shell.
- TPDPWFILE_PRIMARY - 3PAR InServ Storage Server CLI user password file to be used to connect to the InServ Storage Server node from the primary host. This parameter is required if RSH is specified as remote shell.
- TPDPWFILE_BACKUP - 3PAR InServ Storage Server CLI user password file to be used to connect to the InServ Storage Server node from the backup host. This parameter is required if RSH is specified as remote shell.
- VCDBA_MAXVC - The maximum number (500) of the database virtual copies allowed at any time.
- VCDBA_RM_OLDVC - The flag indicates if an oldest virtual copy should be removed before creating a new virtual copy when the number of virtual copies exceeds the maximum allowed.
- LDATAGROUP - The name of the Remote Copy group, which contains Oracle datafile volumes, on the primary (local) InServ Storage Server.

- LARCHGROUP - The name of the Remote Copy group, which contains Oracle archive log volumes, on the primary (local) InServ Storage Server. In a Remote Copy configuration, Oracle datafile volumes and archive log volumes are in the same Remote Copy group. Therefore, this parameter can be left empty.
- LTARGET - The target group name on the primary (local) InServ Storage Server. Use the InForm CLI `showrcopy target` command to get the target name.
- RTARGET - The target group name on the secondary (remote) InServ Storage Server. Use the InForm CLI `showrcopy target` command to get the target name.
- BACKTOOL - The backup method to be used for backing up a database virtual copy (snapshot). The two backup methods currently supported by 3PAR Recovery Manager are NBU backup and RMAN backup. If the specified database is an ASM-managed database, the only supported backup method is RMAN backup.
- NBU_MASTER_SERVER - The Veritas NBU master server.
- DBFILE_CLASS_NAME - The Veritas NBU class (policy) name for backing up database files.
- ARCH_CLASS_NAME - The Veritas NBU class (policy) name for backing up archive logs.
- DBFILE_SCHED_FULL - The Veritas NBU schedule name for backing up database files.
- ARCH_SCHED_FULL - The Veritas NBU schedule name for backing up archive logs (full backup).
- ARCH_SCHED_FULL - The Veritas NBU schedule name for backing up archive logs (incremental backup).
- RMAN_CONN_STR - The RMAN connection string for connecting to the Oracle Recovery Catalog from both the primary host and the backup host.
- RMAN_CHANNEL_TYPE - The RMAN channel type is either SBT_TAPE or DISK.
- RMAN_NO_CHANNEL - The number of RMAN channels to be allocated during backup and restore.
- RMAN_BACKUP_DEST - The backup destination to store RMAN backup image. This option is only required if the specified RMAN channel type is DISK.
- RMVC_AFTER_BACKUP - Specifies whether the virtual copy should be removed after a successful backup.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database

Administrator user must exist on the backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding hostname of the primary host where the specified Oracle database instance is running.

COMMAND

```
vcdba_create
```

SYNOPSIS

```
vcdba_create -s <oracle_sid> -p <primary_host>
[-o online|offline|datafile|archonly] [-v]
```

DESCRIPTION

Creates a virtual copy of a database instance.

The `vcdba_create` command can be used to create an online or offline virtual copy of an Oracle database, a datafile only virtual copy, or an archive log virtual copy.

- Online or offline virtual copy - A consistent point-in-time snapshot image of the database while it is OPEN (online) or CLOSED (offline), respectively.
- Datafile only virtual copy - A snapshot image of all datafiles, not include archive log destinations, of the database while it is OPEN. A virtual copy create with the `-o datafile` option is only useful when archive logfiles generated during the creation of the virtual copy are also available. You may wish to create separate virtual copies using the `-o archonly` option, or use another method to backup archive log destinations.
- Archive log virtual copy - A snapshot image of the archive log destination only.

Once created, the virtual copy can be mounted on the backup host for off-host processing purposes such as backup and database cloning.

A database virtual copy consists of multiple virtual copies of underlying 3PAR virtual volumes used by the Oracle datafiles and/or archive log destination depending on which option is specified (`online`, `offline`, `datafile`, or `archonly`). An archive log virtual copy can be used in conjunction with online or offline virtual copies to simulate an incremental backup.

If Recovery Manager is configured to use Oracle RMAN for backup, an RMAN Recovery Catalog must have been created and configured prior to running this command. The `vcdba_create` command will initiate an RMAN catalog synchronization during the virtual copy creation process.

To use the `vcdba_create` command, the Oracle database structure must satisfy the following requirements:

- The database must be running in archive log mode and automatic archival must be enabled in order to create an online, datafile, or archive log virtual copy.

- If archive log mode is enabled, the data files and archive logs must reside on separate 3PAR virtual volumes.
- The online redo logs and control files should not reside on the same 3PAR virtual volumes used by the data files and archive logs to avoid being restored when using Recovery Manager Rollback feature. However, the online redo logs and control files can share the same 3PAR virtual volumes.
- If the database files reside on Veritas VxVM volumes, the datafiles and archive logs must reside on separate VxVM disk groups. The online redo logs and control files should reside on separate VxVM volumes used by the datafiles and archive logs.
- If the Oracle database is an ASM-managed database, the data files and archive logs must reside on separate ASM disk groups. The online redo logs and control files should not reside on the same ASM disk groups used by the datafiles and archive logs to avoid being restored when using the Recovery Manager Rollback feature. In addition, ASM disk groups should not be shared between different databases.
- If the Oracle database is an RAC database, all RAC instances must share the same archive log destinations (i.e., the same cluster file system or the same ASM disk groups).
- If the database files are symbolic links pointing to actual files and the links do not reside on the same file systems as the actual files, only the actual files are backed up. Otherwise, only the first links and the actual files are backed up; intermediate links will not be backed up.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance ID of the primary database. For an RAC database, any instance ID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-o online` - Creates an online virtual copy of an Oracle database while it is OPEN (online). The specified Oracle database instance must be OPEN. If the database is an RAC database, other database instances can be either OPEN or CLOSED. All tablespaces (or database) will

be put into backup mode before virtual copies of the data file virtual volumes are created. All tablespaces (or database) will then be taken out of backup mode. A log switching will be performed before virtual copies of archive log virtual volumes are created. If the `online`, `offline`, `datafile`, or `archonly` options are not specified, an online virtual copy will be created by default.

- `-o hotbkup` - This option is the same as the `-o online` option and is deprecated. This option will be removed in a future release.
- `-o offline` - Creates an offline virtual copy of an Oracle database while it is CLOSED (offline). The specified database instances must be CLOSED. If the database is an RAC database, all RAC instances must be CLOSED. For this option, only virtual copies of datafile virtual volumes are created.
- `-o coldbkup` - This option is the same as the `-o offline` option and is deprecated. This option will be removed in a future release.
- `-o datafile` - Creates a virtual copy for all datafiles of an Oracle database. The specified Oracle database instance must be OPEN. If the database is an RAC database the other database instances can be either OPEN or CLOSED. All tablespaces (or database) are put into backup mode before virtual copies of the data file virtual volumes are created. All tablespaces (or database) are then taken out of backup mode. A log switching is performed before and after the virtual copy is taken.
- `-o archonly` - Creates a virtual copy of archive log destination only. The specified database instance must be OPEN. If the database is an RAC database, other RAC instances can be either OPEN or CLOSED. A log switching is performed before virtual copies of archive log virtual volumes are created.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

```
vcdba_createdb
```

SYNOPSIS

```
vcdba_createdb -s <oracle_sid> -p <primary_host> -t <timestamp>
[-n <clone_sid>] [-h <clone_ora_home>]
[-o ascii|binary|for_backup[,recovery|norecovery]] [-d <loc>] [-v]
```

DESCRIPTION

Creates a new database instance from a virtual copy.

The vcdba_createdb command creates a fully functional single-instance database or starts up a clone database in MOUNTED mode for RMAN backup purposes. The fully functional single-instance database can be used for any off-host processing purpose. The clone database that is started in MOUNTED mode can only be used for RMAN backup.

The virtual copy used for cloning a database must be either an online or offline virtual copy (created using the online or offline option), respectively. The virtual copy must have been mounted prior to running this command.

You can create a clone database using an ascii or binary controlfile which was saved in the Recovery Manager repository at the time the virtual copy was created. Using an ascii controlfile is more flexible as it allows to change database instance name as well as the structure of the database.

When using an ascii controlfile, the structure of the clone database is not required to be exactly the same as the structure of the primary (original) database. Therefore the virtual copy can be mounted at any mount point. However, since the virtual copy does not contains online redo logs and control files, their locations can be specified using -d option (can be one or more directories or ASM diskgroups, depends on desired multiplexing). If the locations of the redologs and controlfiles are not specified, they are created at the repository location for the virtual copy (/etc/3par/solutions/<*host*>.ora.<*sid*>/<*vc_name*>).

When using a binary controlfile. The structure of the clone database must be exactly the same as the structure of the primary database. Therefore, the virtual copy must be mounted at '/' if the datafiles and archive logs are on file systems. Also, since the virtual copy does not contain redologs and archivelogs, the same directory structure or same ASM diskgroups for redologs and controlfiles must be pre-created on the backup host.

When creating a clone database for backup (RMAN) purposes, the database is started in MOUNTED mode using the binary controlfile from the repository without recovering the database. This can be achieved by using `-o for_backup` or `-o binary,norecovery` option.

A clone database can be created with or without automatic recovery (applying archivelogs from the virtual copy) using `–o recovery` or `-o norecovery` option, if recovery is chosen, the clone database is open with reset log, otherwise, the clone database is in mounted status.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on the backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy. It is also the name of the virtual copy. The virtual copy name can be obtained using the `vcdba_display` command.
- `-n <clone_sid>` - The new Oracle SID for the clone database. If this option is omitted or is used with the `-o for_backup` option, the clone database will have the same `ORACLE_SID` as the primary database. If creating a clone database with the `-o binary` option, the new Oracle SID will be ignored.
- `-h <clone_oracle_home>` - The Oracle home directory on the backup host. If specified, this value will be used instead of the value of the parameter `ORACLE_HOME_BACKUP` in the configuration file.
- `-d <loc>` - A comma-separated list of directories or ASM diskgroups (for multiplexing) to store the new online redologs and controlfiles of the clone database. The directories or ASM diskgroups must have enough available space to hold new online redo logs and controlfiles. Users who run this command must have write permission to this directory or directories. The number of multiplex redo log locations must be equal to or less than the primary database when creating a clone database. Otherwise, the extra redo log multiplex location will be ignored.

- `-o ascii` - Use an ascii controlfile which was saved in the Recovery Manager repository to create a clone database.
- `-o binary` - Use a binary controlfile which was saved in the Recovery Manager repository to create a clone database.
- `-o for_backup` - Use an binary controlfile which was saved in the Recovery Manager repository to create a clone database. The clone database is started in MOUNTED mode without recovery for backup (RMAN) purpose. This option is equivalent to `-o binary,recovery`. This option is deprecated and will be removed in the future release.
- `-o recovery` - Automatically recover the clone database using all available archivelogs that exist on the virtual copy.
- `-o norecovery` - Startup the clone database in mounted mode without recovery.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

`vcdba_display`

SYNOPSIS

```
vcdba_display -s <oracle_sid> -p <primary_host> [-t <timestamp>]
```

DESCRIPTION

Displays virtual copies.

The `vcdba_display` command displays database virtual copies, along with other information including creation time, type, status and backup status.

A virtual copy's type can be either `Online`, `Offline`, `Datafile`, or `Archlog`.

- `Online` or `Offline` virtual copy - Indicates that the virtual copy was created for the database while it was OPEN (online) or CLOSED (offline), respectively.
- `Datafile` virtual copy - Indicates that the virtual copy was created for data files only while the database is open.
- `Archlog` virtual copy- Indicates that the virtual copy was created for the archive log destination only.

A virtual copy's status can be `Available`, `Removed`, `Mounted`, `Mounted(P)`, or `Database`. `Available` status indicates that the virtual copy exists and is not currently mounted or cloned. `Removed` status indicates that the virtual copy is removed. `Mounted` status indicates that the virtual copy is currently mounted. `Mounted(P)` status indicates that the virtual copy is partially mounted. Finally, the `Database` status indicates that a database has been cloned using the virtual copy.

A virtual copy's backup status can be either Y or N, where `Y` indicates that the virtual copy has been backed up, and N indicates that the virtual copy has not been backed up.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy. It is also the name of the virtual copy. The default behavior is to display all virtual copies.

EXAMPLES

- `vcdba_display -s TEST920 -p pilot`.

```
 #  Name         Create Time              Type    Status    Backup?
============ ======================== ======= ========= ========
1. 012403154751 Fri Jan 24 15:47:51 2003 Offline  Available    N
2. 012403154650 Fri Jan 24 15:46:50 2003 ArchLog  Available    N
3. 012403153912 Fri Jan 24 15:39:12 2003 Online   Available    N
4. 012303174743 Thu Jan 23 17:47:43 2003 Datafile Available    N
5. 012303171935 Thu Jan 23 17:19:35 2003 ArchLog  Available    N
```

- `vcdba_display -s TEST920 -p pilot -t 012405154751`

```
 #  Name         Create Time              Type   Status    Backup?
============ ======================== ====== ========= ========
1. 012403153912 Fri Jan 24 15:39:12 2003 Online Available   N

     Virtual Copy's Content:
             /demo/data/system01.dbf
             /demo/data/tools01.dbf
             /demo/data/rbs01.dbf
             /demo/data/temp_df.dbf
             /demo/data/users01.dbf
             /demo/data/users02.dbf
             /demo/arch
```

COMMAND

```
vcdba_export
```

SYNOPSIS

```
vcdba_export -s <oracle_sid> -p <primary_host> -r alt_host
-t <timestamp> [-l <alt_tpdhost>] -e alt_tpdpwfile|alt_tpdusername [-v]
```

DESCRIPTION

The vcdba_export command exports a virtual copy's repository from the current backup host to an alternate backup host. The exported virtual copy can then be mounted or cloned at the alternate backup host. A virtual copy's repository can be exported to multiple alternate backup hosts, which share the same InServ Storage Server as the original backup host. A virtual copy can only be mounted on one backup host at a time.

The first time a virtual copy repository is exported to an alternate backup host, the vcdba_export command also copies the Recovery Manager configuration file from the current backup host to the alternate backup host.

The vcdba_export command also modifies configuration parameters according to the values specified in the arguments for alt_tpdhost, alt_tpdpwfile, and alt_tpdusername.

If the vcdba_export command is invoked by an Oracle DBA, an identical Oracle user ID and group ID must exist on the alternate backup host.

If SSH is currently configured for accessing from the current backup host to the primary host and the InServ Storage Server, then SSH must also be configured to allow accessing from the current backup host to the alternate backup host as well as from the alternate backup host to the InServ Storage Server. SSH is the only supported remote access method on Linux systems by 3PAR Recovery Manager.

If RSH and CLI are configured to access from the current backup host to the primary host and the InServ Storage Server, then RSH and CLI must also be configured to allow access from the current backup host to the alternate backup host, as well as from the alternate backup host to the InServ Storage Server.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator to run this command, an identical Oracle Database Administrator user must exist on alternate backup host. In addition, permission on the /opt/3par/vcdbaora directory must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance ID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy. It is also the name of the virtual copy. The virtual copy name can be obtained using the `vcdba_display` command.
- `-r <alt_host>` - The alternate backup host name.
- `-l <alt_tpd_hostname>` - The TPD hostname is the hostname defined on the InServ Storage Server, which represents the alternate backup host. The `showhost` command lists all available TPD host names.
- `-e alt_tpdpwfile|alt_tpdusername`
  - `alt_tpdpwfile` - The location of the 3PAR InServ Storage Server client password file that will be used by Recovery Manager to access the InServ Storage Server from the alternate backup host. The password file can be created using InForm CLI `setpassword` command.
  - `alt_tpdusername` - The 3PAR InServ Storage Server username that will be used by Recovery Manager to connect to the InServ Storage Server from the alternate backup host. The InServ Storage Server user can be created using the InForm CLI `createuser` command. The created user must have `edit` or above privilege.
  - If the InForm CLI is configured to allow access from the alternate backup host to the InServ Storage Server, then `alt_tpdpwfile` must be specified. If SSH is configured to allow access from the alternate backup host to the InServ Storage Server, then `alt_tpdusername` must be specified.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

`vcdba_main`

SYNOPSIS

`vcdba_main`

DESCRIPTION

The `vcdba_main` command provides a menu-driven interface to perform 3PAR Virtual Copy administration for off-host backup and off-host processing.

Each menu contains the necessary steps to guide you through the process to perform the corresponding task. Each step may require user's interaction.

- Each menu page contains a standard menu selection.

  ? - Provide help page for the current working menu

  r - Return to the previous

  x - Exit from the program

- The main menu provides following selection:

  1 - Configuration Administration

  Use this menu to setup a configuration file per database instance.

  - Create A Backup Configuration
  - List All Backup Configuration
  - Update A Backup Configuration
  - Remove A Backup Configuration

  2 - Virtual Copy Management

  Use this menu to perform all actions of a virtual copy. To display/create/remove/mount/unmount virtual copy, use the remove virtual copy repository menu selection to remove a virtual copy permanently, as well as setting up the policy of the virtual copy.

  - Display Virtual Copy
  - Create Virtual Copy
  - Remove Virtual Copy

- Mount Virtual Copy

- Unmount Virtual Copy

- Export Virtual Copy

- Remove Virtual Copy Repository

Each virtual copy created by Recovery Manager will keep information in the repository to allow restore from tape or disk successfully even the associate virtual copy has been removed. Once the virtual copy is no longer needed, use this selection to free up repository space.

- Virtual Copy Policy

Allow the maximum number of virtual copy setting per database instance. Remove or retain the oldest virtual copy when the maximum number is reached.

3 - Backup Administration

Use this menu to backup the existing virtual copy to tape or disk, or perform Virtual Copy creation for off-host backup or off-host processing.

- Backup Database

- Backup Archive Logs

4 - Restore Administration

Use this menu to perform restore from a virtual copy backup image. You can use this menu only if virtual copies are backed up by Veritas NetBackup using the 3PAR Backup Administration menu.

5 - Remote Copy Administration

Use this menu to perform periodic synchronization for virtual volumes used by a database.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

COMMAND

`vcdba_mount`

SYNOPSIS

```
vcdba_mount -s <oracle_sid> -p <primary_host> -t <timestamp>
[-m <mountpoin>t] [-r] [-v]
```

DESCRIPTION

Mounts a virtual copy.

The `vcdba_mount` command mounts an existing virtual copy created by the `vcdba_create` command on the backup host. The mounted virtual copy can be used for off-host processing purposes such as backup or database cloning.

The following restrictions apply when mounting a database virtual copy:

- The virtual copy must have an `Available` or `Mounted(P)` status in order to be mounted. The virtual copy's status can be retrieved using the Recovery Manager display utility.
- The same virtual copy cannot be mounted concurrently at different mount points.
- If the database files reside on Veritas VxVM Volumes, only one virtual copy per database can be mounted at any time on the backup host. This is due to the VxVM disk groups from different virtual copies of the same database having the same names and so cannot be imported at the same time.
- If the database files reside on ASM disk groups, it is dependent on which ASM database version is installed on the backup host, different restrictions apply as follows:
  - If the ASM versoin on the backup host is 10.2.0.5 or 11.1.0.7, one virtual copy per database can be mounted on the backup host. Virtual copies from different databases can be mounted concurrently.
  - If the ASM vesrion on the backup host is running versions lower than the releases mentioned in the previous bullet, only one virtual copy can be mounted at any time on the backup host. This restriction prevents an Oracle ASM instance on the backup host from hanging due to some ASM's idle processes still holding a virtual copy's devices, even though the corresponding ASM disk groups are dropped.
- If the database files reside on OCFS2 file systems, only one virtual copy per database can be mounted at any time on the backup host.

Mounting a database virtual copy involves the following actions:

- Creates a read-write virtual copy the original read-only virtual copy.
- Imports the read-write virtual copy to the backup host.
- Imports snapshot VERTIAS VxVM disk groups and starts up all corresponding snapshot VxVM volumes if the database files reside on VxVM volumes.
- For virtual copies from an ASM-managed database, based on the different ASM database releases on the backup host, the operation is different.
  - For ASM versions 10.2.0.5 or 11.0.1.7, if an ASM instance exists and is up on the backup host, then all diskgroups from the virtual copy are mounted in this ASM instance. Otherwise, an ASM instance is started up on the backup host, and all ASM disk groups in the virtual copy are mounted.
  - For ASM versions lower than the releases mentioned in the previous bullet, if an ASM instance is up on the backup host, the mount utility checks if there is any mounted diskgroup. If none, the ASM instance is shut down, otherwise, the mount utility gives an error and exits. After that, a new ASM instance is started up and all diskgroups contained in the current virtual copy are mounted.
- Mounts all snapshot file systems if the database files reside on file systems.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy. It is also the name of the virtual copy. The virtual copy name can be obtained using the `vcdba_display` command.

- `-m <mountpoint>` - The destination location where the virtual copy is mounted. The current user must have permission to write to this location. By default, the virtual copy will be mounted at `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/<timestamp>`. If ASM is used on the backup host, this option will be ingnored.
- `-r` - Re-mounts a virtual copy that has previously been mounted, but has been un-mounted due to system reboot. This option is also helpful where a virtual copy has previously been partially mounted, but the virtual copy devices must be scanned manually if the host HBA is Egenera.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

vcdba_remove

SYNOPSIS

```
vcdba_remove -s <oracle_sid> -p <primary_host> -t <timestamp> [-v]
```

DESCRIPTION

Removes a virtual copy.

The vcdba_remove command removes a virtual copy created by the vcdba_create command. The virtual copy must have Available status in order to be removed. The status of the virtual copy can be retrieved using the vcdba_display command.

If the specified virtual copy has been backed up, the actual database virtual copy is removed, but its repository remains for database restoration purposes. To remove the virtual copy's repository, use the vcdba_rmrep command. If the virtual copy's repository is removed, Recovery Manager will not be able to perform a database restore operation even if the virtual copy has been backed up.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- -s <oracle_sid> - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- -p <primary_host> - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the hostname command.
- -t <timestamp> - The timestamp of a virtual copy. It is also the name of the virtual copy. The virtual copy name can be obtained using the vcdba_display command.
- -v - Runs the command in verbose mode to display useful messages.

COMMAND

vcdba_removedb

SYNOPSIS

```
vcdba_removedb -s <oracle_sid> -p <primary_host> -t <timestamp>
[-n <clone_sid>] [-h <clone_oracle_home>] [-f] [-v]
```

DESCRIPTION

The vcdba_removedb command removes a clone database that was created using the vcdba_createdb command.

The clone database is shutdown with the shutdown immediate option. All files (Oracle parameter file, control files, and redo logs), previously created with the vcdba_createdb command are removed. The virtual copy remains mounted.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- -s <oracle_sid> - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- -p <primary_host> - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the hostname command.
- -t <timestamp> - The timestamp of a virtual copy that was previously used to create the clone database.
- -n <clone_sid> - The instance ID of the cloned database to be removed. If the clone database uses the same <oracle_sid> as the primary <oracle_sid>, this option can be omitted.

- `-h <clone_oracle_home>` - The Oracle home directory of the cloned database on the backup host. If specified, this value is used instead of the value of the `ORACLE_HOME_BACKUP` parameter in the configuration file.
- `-f` - Forces the removal of the clone database.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

```
vcdba_restore
```

SYNOPSIS

```
vcdba_restore -s <oracle_sid> -p <primary_host> [-t <timestamp>]
[-T <tablespaces>|-D <datafiles>] [-h hostname] [-m alt_mountpoint]
[-c] [-v]
```

DESCRIPTION

Restores database files from a virtual copy backup image.

The vcdba_restore command restores databases, tablespaces, data files, and/or archive logs from a virtual copy backup image. The virtual copy must have a status of Y in order to be restored. The virtual copy's backup status can be retrieved using the vcdba_display command.

The command can also be used to restore a virtual copy's backup image to an alternate backup host. For NBU (user-managed) restoration, the command can also be used to restore an alternate location. Oracle RMAN always restores to the primary host.

If a virtual copy's name is not specified, the vcdba_restore command restores from the most recent full back up.

Restore is not supported on Remote Copy Configuration.

Restore is not supported on Remote Copy configuration.

The following restrictions apply when restoring from a virtual copy's backup image:

- When restoring the database control file (using the -c option) using Oracle RMAN, the database must be in STARTED mode (startup nomount). In addition, restoring the database control file along with an individual data file or tablespace is not supported, as it is not possible to perform media recovery.
- When restoring a database, the database must be in CLOSED or MOUNTED mode for NBU restore or Oracle RMAN restore, respectively. For an RAC database, all RAC instances must be in CLOSED or MOUNTED mode, respectively.
- When restoring individual tablespaces or datafiles, the database can be OPEN, but the corresponding tablespaces must be offline.
- Restoring controlfiles along with datafiles and/or tablespaces is not allowed.

- If the database is an ASM managed database, all ASM disk groups must be mounted prior to running this command.
- For NBU (user-managed) restore, a file named `/usr/openv/netbackup/db/altnames/<database_hostname>` must be created on the NBU master server in order to perform restoration to a host (including the primary host) that differs from the backup host. `<database_hostname>` is the host name of the database server to restore.

Depending on the type of the virtual copy backup image (online, offline, datafile, or archonly), corresponding database files are restored appropriately.

For NBU (user-managed) restore:

- Control files are not restored by default.
- For an online virtual copy, both data files and archive logs are restored unless individual tablespaces or data files are specified. In this case, only the corresponding data files are restored.
- For an offline virtual copy, only data files are restored.
- For a datafile only virtual copy, only data files are restored.
- For an archive log virtual copy, only archive logs are restored.

For Oracle RMAN restore:

- Control files are not restored by default.
- For an online virtual copy, only data files are restored. Archive logs are not restored to minimize restoration time. Oracle RMAN can restore necessary archive logs during recovery (refer to Oracle documentation for details on how to use Oracle RMAN for recovery).
- For an offline virtual copy, only data files are restored.
- For a datafile-only virtual copy, only data files are restored.
- For an archive log virtual copy, archive log restoration is not supported as Oracle RMAN can restore necessary archive logs during recovery (refer to Oracle documentation for details on how to use Oracle RMAN for recovery).

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

Only the super user or the owner of the virtual copy can restore the specified virtual copy.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy whose backup image is used for restoration. Use the `vcdba_display` command to retrieve a list of the virtual copy names. If a name is not specified, the most recent virtual copy's backup (full) image is used for the restoration.
- `-T <tablespaces>` - The tablespace(s) that need to be restored. Use commas to separate multiple tablespace names.
- `-D <datafiles>` - The datafile(s) that need to be restored. Use commas to separate multiple datafiles.
- `-h <hostname>` - The host name to restore to. If this option is omitted, the virtual copy's backup image is restored to the primary host by default.
- `-m <mountpoint>` - The mount point to restore to. If this option is omitted, the virtual copy's backup image is restored to its original location by default.
- `-c` - Indicates that the control files are restored. If this option is omitted, the control files are not restored by default. Restoring controlfiles along with datafiles and/or tablespaces is not supported.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

`vcdba_rmrep`

SYNOPSIS

```
vcdba_rmrep -s <oracle_sid> -p <primary_host> [-t <timestamp>]
[-f] [-v]
```

DESCRIPTION

Removes a virtual copy repository.

The `vcdba_rmrep` command removes a virtual copy repository, specified by the `<timestamp>` parameter. If the `<timestamp>` is not specified, the entire database repository will be removed.

If removing a virtual copy repository, the virtual copy's status must be `Removed` and its backup status must be N. If the virtual copy’s status is Y, the `-f` option can be used to force the removal of the repository. The virtual copy's status and backup status can be obtained using the `vcdba_display` command.

If removing a database repository, all of the existing virtual copies and their repositories must be removed first.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy whose repository is to be removed. The virtual copy name can be obtained using `vcdba_display` command. If the `<timestamp>` is not specified, the entire repository will be removed.

- `-f` - Forces the removal of the virtual copy repository even if the virtual copy has been previously backed up.
- `-v` - Runs the command in verbose mode to display a useful messages.

COMMAND

```
vcdba_rollback
```

SYNOPSIS

```
vcdba_rollback -s <oracle_sid> -p <primary_host> -t <timestamp>
[-o data|arch] [-v] [-w] [-f]
```

DESCRIPTION

Rolls back database volumes from an online virtual copy.

The `vcdba_rollback` command promotes a virtual copy's volumes back to their base virtual volumes. The base virtual volumes used by the database are rolled back to the virtual copy's volumes. Once the promote (rollback) process completes successfully, the base virtual volumes will be exactly the same as the virtual copy's volumes. If the base volume size has been changed since the virtual copy was taken, the rollback process will not affect the new size.

When rolling back from an online virtual copy, both datafile and archive log virtual volumes are rolled back by default. Use the `-o` option to roll back only datafile virtual volumes or only archive log virtual volumes.

When rolling back from an offline virtual copy, only datafile virtual volumes are rolled back.

When rolling back from an archive log virtual copy, only archive log virtual volumes are rolled back.

The following restrictions apply when rolling back a virtual copy:

- The online redo logs and control file should not reside on the same virtual volumes used by the datafiles and archive logs. Otherwise, they will be rolled back along with the datafile and archive log virtual volumes.
- The database instance must be CLOSED for this operation. If the database is an RAC database, all RAC instances must be CLOSED.
- The base (data file and/or archive log) virtual volumes must not be exported.
- The specified virtual copy must have an `Available` (not mounted) status.
- If the base virtual volumes are involved in a Remote Copy group you must use `-f` to promote the virtual copies back to their base volumes.

Recovery Manager saves an ACII control file and a binary control file for each created virtual copy in its repository. After a rollback, you may need to restore the control file in order to perform database recovery.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on the backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy form which to promote. The virtual copy name can be obtained using the `vcdba_display` command.
- `-o [data|arch]`
  - `data` - Promotes only the virtual copy's datafile volumes back to their base virtual volumes.
  - `arch` - Promotes only the virtual copy's archive log volumes back to their base virtual volumes.
- `-v` - Runs the command in verbose mode to display useful messages.
- `-w` - Promotes the read-write virtual copy instead of the read-only virtual copy back to its base. The default is to promote the read-only virtual copy.
- `- f` - Forces the promote operation to proceed even if the parent base volumes are currently in a Remote Copy group, as long as the Remote Copy group has not been started. If started, the promote will fail.

COMMAND

`vcdba_rsync`

SYNOPSIS

```
vcdba_rsync -s <oracle_sid> -p <primary_host>
[-o online|offline|checkonly] [-v]
```

DESCRIPTION

The `vcdba_rsync` command performs a periodic synchronization for database virtual volumes. During synchronization, changed data from the virtual volumes on the primary/local InServ Storage Server is pushed over to the corresponding remote virtual volumes on the secondary/remote InServ Storage Server.

Once the synchronization process completes, the `vcdba_rsync` command automatically creates virtual copies of the corresponding virtual volumes on the secondary/remote InServ Storage Server and presents itself to the user as one database virtual copy.

The `vcdba_rsync` command can be used to perform periodic synchronization for datafile and archive log virtual volumes, or datafile virtual volumes.

In the previous release, 3PAR Recovery Manager required that two Remote Copy groups had to be created. One contained all data file volumes and one contained archive log volumes. In the current release, 3PAR also supports one Remote Copy group, which contains both datafile volumes and archive log volumes.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-o online` - Performs periodic synchronization for datafile and archive log virtual volumes while the database is OPEN.
- `-o hotbkup` - This option is the same as the `-o online` and is deprecated. This option will be removed in a future release.

- `-o offline`- Performs periodic synchronization for datafile virtual volumes while the database is CLOSED.
- `-o coldbkup` - This option is the same as the `-o offline` and is deprecated. This option will be removed in a future release.
- `-o checkonly` - Verifies the Remote Copy configuration.
- `-v` - Runs the command in verbose mode to display useful messages.

COMMAND

vcdba_umount

SYNOPSIS

```
vcdba_umount -s <oracle_sid> -p <primary_host> -t <timestamp>
[-f ] [-v]
```

DESCRIPTION

Unmounts a virtual copy.

The vcdba_umount command unmounts a mounted database virtual copy. The virtual copy must have Mounted or Mounted(P) status in order to be unmounted. The virtual copy unmounting process only removes the read-write virtual copy; the read-only virtual copy remains intact.

Unmounting a database virtual copy involves the following actions:

- For an ASM-managed database, if the ASM version on the backup host is 10.2.0.5 or 11.1.0.7, unmounting the virtual copy drops the ASM diskgroups that are contained in the virtual copy and cleans up the ASM disks.
- If the ASM version on the backup is lower than those listed in the previous bullet, unmounting shuts down the ASM instance and cleans up ASM disks.
- Unmounts all snapshot file systems if the database files reside on file systems.
- Destroys all snapshot VxVM disk groups and their VxVM volumes if the database files reside on VxVM volumes.
- Deports the read-write virtual copy from the backup host.
- Removes the read-write virtual copy.

You must run this command as a super user from the backup host. To allow the Oracle Database Administrator (Oracle Owner) to run this command, an identical Oracle Database Administrator user must exist on backup host. In addition, permission on the 3PAR Recovery Manager Installation and Repository directories must be changed appropriately.

OPTIONS

The following options are supported:

- `-s <oracle_sid>` - The instance SID of the primary database. For an RAC database, any instance SID can be specified.
- `-p <primary_host>` - The corresponding host name of the primary host where the specified Oracle database instance is running. The value of the primary host name must match the output of the `hostname` command.
- `-t <timestamp>` - The timestamp of a virtual copy to be unmounted. The virtual copy name can be obtained using the `vcdba_display` command.
- `-f` - Forcibly unmounts a database virtual copy. Without this option, the `vcdba_umount` command does not allow a virtual copy to be unmounted if it is being used. Using this option can corrupt the corresponding read-write virtual copy. However, the read-only virtual copy remains intact. This option is useful in cases where the virtual copy is partially mounted due to mounting failure.
- `-v` - Runs the command in verbose mode to display useful messages.

7
Using the Recovery Manager Graphical User Interface

In this chapter

7.1 Starting and Stopping the Recovery Manager GUI

The 3PAR Recovery Manager Graphical User Interface (GUI) is installed when the VCDBAora package is installed.

7.1.1 Starting the GUI

To start the Recovery Manager GUI:

1. Ensure that the DISPLAY environment variable is set.
2. Verify that the X11 server is running on the destination host where the GUI is displayed. If the X11 server is not running, enter the following command:

   For Solaris:

```
/usr/openwin/bin/xhost +
```

   For Linux:

```
/usr/X11R6/bin/xhost +
```

3. Type the following command in an open terminal:

```
/opt/3par/vcdbaora/bin/vcdbagui
```

4. Press ENTER.

NOTE: It is a known issue that the mouse events are not captured correctly on the cywin x-server for Java6.

7.2 Stopping the GUI

- To stop the Recovery Manager GUI, click **Console** and then **Exit**.

7.3 Creating Configuration Files

3PAR Recovery Manager relies on configuration files for most of its operations. There are two types of configuration files, Recovery Manager with Remote Copy and Recovery Manager without Remote Copy. The Recovery Manager repository is located in the `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>` directory on the backup host.

Refer to *4.9 Recovery Manager Configuration Files* on page 4.27 for additional details on creating configuration files with or without the Remote Copy feature.

NOTE: The configuration file cannot be recreated if it already exists in the repository. You can modify the configuration as needed, or remove the configuration before a new one can be created.

7.4 Modifying Configuration Files

Configuration files can only be modified from the host node level. Modifications are made in the `config` and `config_exp.sh` files in the repository.

7.5 Removing Configuration Files

Configuration files can be removed if there are no virtual copies existing in the repository. When configuration files are removed, the entire repository is also removed.

7.6 Using Virtual Copies

7.6.1 Creating a Virtual Copy

This feature supports hot (online) and cold (offline) backup of a database instance or backup of archive log destinations only.

Creating a virtual copy requires the primary host Oracle SID. Perform this function through the menu, tool bar, and popup menu.

To create a virtual copy, perform the following procedure:

1. Select **Virtual Copy Management** from the navigation view.
2. Select **Create Virtual Copy** from the **Virtual Copies** pull-down menu.
3. Select the desired options (online backup, offline backup, backup datafile only, or backup archive log dest only) from the dialog box.
    - **Online (Hot) backup** - The involved database instance must be up for this operation. All tablespaces are put in backup mode before the virtual copy is created. After the virtual copy creation is completed, tablespaces are taken out of backup mode.
    - **Offline (Cold) backup** - The involved database instance must be down for this operation.
    - **Backup datafile only** - The involved database instance must be up for this operation. All tablespaces are put in backup mode before the virtual copy is created. After the virtual copy creation is completed, tablespaces are taken out of backup mode. This backup only takes a virtual copy for all datafiles; not archive log destination. A virtual copy created with the `-o datafile` option is only useful when archive logfiles generated during the creation of the virtual copy are also available. You may want to create separate virtual copies using the `-o archonly` option.
    - **Backup Archive Log Dest Only** - The involved database instance must be up for this operation. The database is forced to switch logs before a virtual copy of archive logs is created.
4. Click **Finish**.

7.6.2 Setting up Virtual Copy Policy

This feature allows the control of the number of virtual copies on an InServ Storage Server. When the maximum number of virtual copies is reached, the oldest copy can either be removed or retained.

To create a virtual copy policy, perform the following procedure:

1. Select **Virtual Copy Management** from the navigation view.
2. Select the **Virtual Copy Policy** menu from the **Virtual Copies** pull-down menu.
3. Enter the maximum number of virtual copies to be kept in the text field.
4. If you want to remove the oldest virtual copy, select **Remove the oldest Virtual Copy**. If you want to keep the oldest virtual copy, select **Retain the oldest Virtual Copy** option.
    - **Remove the oldest Virtual Copy** - If the maximum number of virtual copies is reached, the oldest virtual copy is removed before a new virtual copy is created.
    - **Retain the oldest Virtual Copy** - If the maximum number of virtual copies is reached, the oldest virtual copy is retained and a new virtual copy is created.
5. Click **Finish**.

NOTE: The virtual copy policy is effective immediately.

7.6.3 Refreshing Virtual Copy Information

You can update virtual copy information that includes Backup Type, Backup Key, Mount point and Virtual Volume State. If a new virtual copy is created outside of the Recovery Manager GUI, the virtual copy is added to the navigation view.

1. Select **Virtual Copy Management** from the navigation view.
2. Select **Refresh** from the **Virtual Copies** pull-down menu.

NOTE: The refresh process begins immediately. It takes a few minutes depending on the number of virtual copies in the Recovery Manager repository.

7.6.4 Mounting a Virtual Copy

After a virtual copy is created, it can be mounted on the backup host where the Recovery Manager GUI is running.

To mount a virtual copy, perform the following procedure:

1. Right-click the virtual copy you wish to mount.
2. Click **Mount**.

   A screen appears showing the virtual copy name, and creation time. You are prompted for the mount point where you want the virtual copy being mounted on the backup host. The default mount point is:
   `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/<timestamp>`
3. Click **Finish**.

   Recovery Manager begins mounting all the file systems for you. When the mounting of the file systems is complete, a screen displays the successful message.
4. Click **OK**.

In the **Virtual Volume State** column, **Mounted** should be displayed indicating that the virtual copies are mounted on the backup host. The mount point is also displayed indicating the location of the mounted file systems.

After a virtual copy is in the **Mounted** state, a database instance can be created on the backup host by cloning the database (see *7.6.12 Cloning a Database* on page 7.9).

7.6.5 Unmounting a Virtual Copy

After a virtual copy is in the **Mounted** state, an unmount operation can be executed.

To unmount a virtual copy:

1. Right-click the virtual copy you wish to unmount.
2. Click **Unmount**.
3. Click **Finish**.

   A successful message shows on screen after it is finished.
4. Click **OK**.

   The **Virtual Volume State** column for this virtual copy changes to **Available**.

7.6.6 Removing a Virtual Copy

After the **Virtual Volume State** column displays **Available**, the virtual copy can be deleted.

CAUTION: Removing a virtual copy permanently removes the virtual copy from the system.

To remove a virtual copy:

1. Right-click the virtual copy you wish to remove.
2. Click **Remove Virtual Copy**.
3. Click **Yes** when prompted for confirmation to remove the virtual copy.

   A successful message shows on screen after it is finished.
4. Click **OK**.

   The virtual copy is removed from the virtual copy management list.

7.6.7 Backing up a Virtual Copy

If a virtual copy is in the **Available** state, it can be backed up. If a virtual copy is in the **Mounted** or **Database** state, the virtual copy needs to be to unmounted prior to being backed up.

To backup a virtual copy:

1. Right-click the virtual copy to be backed up to media.
2. Click **Backup to Media**.
3. Click **Finish**.
4. Click **OK**.

7.6.8 Removing a Virtual Copy Repository

Normally, when the virtual copy is removed, the repository is deleted. However, if you have already backed up the repository is not automatically removed. It is kept to apply the restore operations when necessary. After the virtual copy repository is removed, all information related to this virtual copy set is lost.

1. Right-click the virtual copy name to be removed from the entire repository.

2 Click **Remove Virtual Copy Repository**.

3 Click **Yes** when prompted for confirmation to remove the repository.

The removed repository is no longer displayed on the virtual copy management screen.

7.6.9 Restoring Datafiles

If Veritas NetBackup (NBU) is used to back up datafiles, NBU can be used to restore datafiles to the primary host, backup host, or any other hosts where the NBU clients for the same NBU master server are configured.

If the virtual copy is being backed up using NBU, the backup key has the format: `<oracle_sid>_<primary_host>_<timestamp>`.

To restore a datafile:

1 Right-click the desired virtual copy.

2 Click **Restore**.

A screen appears displaying the virtual copy set information and you are prompted for the host name and mount point for restoring the data files. If the mount point is left blank, files are restored to their original paths on the primary host.

3 Click **Finish**.

7.6.10 Refreshing Database Information

Tablespace, datafile, archive log, and virtual volume information can be refreshed in the Recovery Manager GUI by performing the following:

1 Click any of **Tablespace**, **Datafiles**, **Archive Log**, or **Virtual Volumes** in the left-hand tree.

2 Click **Refresh** in the tool bar.

Recovery Manager retrieves all the information from the primary database.

All mappings are for informational purposes and cannot be modified. All mappings reflect the current database and virtual copy information if the primary database is accessible.

7.6.11 Exporting a Virtual Copy to an Alternate Backup Host

After a virtual copy is created, it can be exported to an alternate backup host.

Export a virtual copy as follows:

1 Right-click the virtual copy you wish to export and click **Export**.

The **Export Virtual Copy** screen appears.

2 On the **Export Virtual Copy** screen, provide the following information:

- **Alternate Backup Host Name -** the name of the backup host to which the virtual copy is exported.
- **InServ Password File** - the location of the InServ Storage Server CLI password at the alternate backup host. This text field will display if RSH is selected.
- **InServ User Name** - the storage server user name for the alternate backup host. This text field will display if RSH is selected.
- **Backup Host Name in InServ** - the alternate backup host name defined in the InServ Storage Server.

3 Click **Finish** to start exporting the virtual copy.

7.6.12 Cloning a Database

Each online virtual copy created by Recovery Manager represents a point-in-time database image. Recovery Manager can use the virtual copy to help restore the database, or to clone the database for testing, decision making, and report generating purposes. The cloning capability takes the workload out of the primary host and reduces performance impact.

In order to create the cloned database from virtual copies, these virtual copies must be created by Recovery Manager with the online or offline database option.

The cloned database is created on the backup host.

To clone a database:

1 Select a virtual copy that has a status of **Mounted**.

2 Right-click the mounted virtual copy and click **Create database**.

3 Provide the new database ID and the Oracle home directory.

4 If an ascii control file is chosen to clone the database (this is default option), provide one or more mount points on the backup host for the control files and the redo log files (control files and redo log files are multiplexed across the mount points).

Example: If you provide `/clone_directory1`, `/clone_directory2`, `+CLONE_DATA` notice combined ASM diskgroup and file systems are allowed in this operation, make sure adequate permissions are granted for the user executing the clone utility. If the binary control file is chosen to clone the database, the clone operation will use exactly the same structure as that in the primary database. The virtual copy must be mounted at '/' before the database creation operation starts in order to ensure the clone database has exactly the same structure for all database files.

5 Click **Finish**.

After the cloned database operation has completed, the **Virtual Volume** column is changed from **Mounted** to **Database** to indicate the cloned database is up and running.

6 Click **OK**.

7.6.13 Removing a Cloned Database

When a cloned database is no longer needed, it can be removed with the following procedure:

1 Select a virtual copy with a status of **Database**.

2 Right-click on the selected virtual copy and click **Remove database**.

3 Click **Yes**.

4 Click **OK**.

7.7 Periodic Database Synchronization

The periodic synchronization process is an asynchronous process. Synchronization takes minutes to hours for the synchronized process to finish depending on data changes, network speed, and load on the primary host, backup host, primary/local and secondary/remote InServ Storage Servers. When the synchronization completes, Recovery Manager creates a virtual copy on the remote (secondary) InServ Storage Server, updates the navigation view, and sends notification to the user.

7.7.1 Starting Periodic Synchronization

To start periodic synchronization on a Remote Copy node:

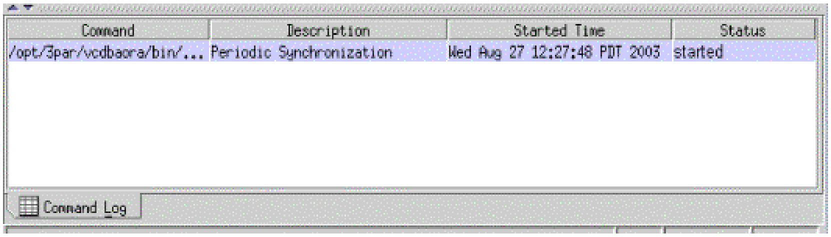
1. Right-click a **Remote Copy** node on the navigation tree and click **Periodic Sync Virtual Volumes**.

   The **Periodic Synchronization Virtual Volumes** screen appears.

> **NOTE:** Recovery Manager does not allow more than one periodic synchronization process for the same database at the same time.

2. Depending on the setup of your database, select either **Online (Hot) Backup** or **Offline (Cold) Backup** and then click **Finish**.

   After the periodic synchronization process is started, the command log view of the Recovery Manager GUI displays a status of **started**.



Command	Description	Started Time	Status
/opt/3par/vcdbaora/bin/...	Periodic Synchronization	Wed Aug 27 12:27:48 PDT 2003	started

7.7.2 Verifying the Periodic Synchronization Process

When starting periodic synchronization on a Remote Copy node, you may wish to verify that the synchronization process is occurring.

- To verify the periodic synchronization on a Remote Copy node, right-click the **Remote Copy** node where synchronization has started and click **Periodic Sync Status**.

  A window appears displaying the status of the synchronization process.

7.7.3 Removing the Recovery Manager Periodic Sync Lock

Recovery Manager does not permit more than one periodic synchronization process for the same database at a time. Recovery Manager uses the Periodic Sync Lock to prevent simultaneous synchronization processes from occurring on a single database.

If Recovery Manager prevents you from performing a periodic synchronization of your Remote Copy group when no other synchronization processes are occurring, the Periodic Sync Lock can be removed.

- ▶ To remove the **Periodic Sync Lock**, right-click the **Remote Copy** node you wish to synchronize and click **Remove Periodic Sync Lock**.

7.7.4 Refreshing Remote Copy Information

After performing periodic synchronization on a Remote Copy node, you need to refresh the Recovery Manager GUI so that the most current information is displayed.

- ▶ To refresh Remote Copy information, right-click the **Remote Copy** node on which synchronization was performed and click **Refresh**.

8 Using the Recovery Manager Rollback Utility

In this chapter

Recovery Manager provides a way to rollback a database to a point-in-time stage with a read-only or read-write virtual copy.

The rollback utility requires the data volumes be offline without being exported to any giving host. Therefore it is very important to keep the original volume numbers from being reused by other volumes. Recovery Manager uses them for creating LUNs and exporting them to the original host with the same set of volume numbers.

8.1 vcdba_rollback Usage

Refer to *vcdba_rollback* on page 6.35 for the syntax and available options for the `vcdba_rollback` command.

The procedure to rollback the data volumes depends on the data type of the datafile. If the datafiles are composed from Veritas VxVM then special VxVM procedures apply.

8.2 Database Volumes Not Under Veritas VxVM Control

If none of the disk volumes used by a database are under Veritas VxVM control, perform the following procedures.

8.2.1 Rollback with Read-Only Virtual Copies

1. On the primary host, shutdown the database if it is up and running. If ASM is being used, unmount all involved ASM disk groups.
2. On the primary host, unmount all file systems where the database volumes are mounted.
3. On the InServ Storage Server, remove the VLUNs for the data volumes by issuing the `removevlun <vvname> <lun> <host>` command.

   Example:

```
removevlun Oracle_data1 101 pilot
```

4. Keep the list of the VLUNs, which are removed by the command above. The VLUNs are used to re-export the LUNs with the same disk IDs after rollback operation is completed.
5. From the backup host, execute the `vcdba_rollback -s <oracle_sid> -p <primary_host> -t <timestamp> -v` command to roll back the read-only copy:

   Example:

```
vcdba_rollback -s TEST920 -p pilot -t 042903142921 -v
```

6. On the InServ Storage Server, export all the data volumes to the primary host with the same VLUNs saved in step 4 by issuing the `createvlun <vvname> <lun> <host>` CLI command:

Example:

```
createvlun Oracle_data1 101 pilot
```

7 On the primary host, run the `fsck` command on all mount points, and then mount each disk to its original mount point. If ASM is being used, mount all involved ASM disk groups.

8 On the primary host, follow Oracle documentation to perform media recovery to recover the database.

8.2.2 Rollback with Read-Write Virtual Copies

The difference between a read-only and a read-write virtual copy depends on whether the read-write virtual copy has been exported and if any I/O operations have been applied on the copy or not.

- For a cloned database on the backup host, you need to perform log switches until all online redo logs are switched to archive log files. The cloned database must then be shut down. All file systems used by the cloned database have to be manually unmounted, and remain offline with the `umount` and `removevlun` commands.

NOTE: Be sure to manually unmount the file systems used by the cloned database on the backup host. Do not use the `vcdba_umount` utility, which not only unmounts the file systems, but also removes the read-write virtual copy from the InServ system.

- In addition to performing the *8.2.1 Rollback with Read-Only Virtual Copies* on page 8.2, use the `-w` option to specify read-write virtual copy in step 3 in *8.2.1 Rollback with Read-Only Virtual Copies* on page 8.2.

8.3 Database Volumes Under Veritas VxVM Control

If any of the database volumes are under Veritas VxVM control, perform the following procedures.

8.3.1 Rollback with Read-Write Virtual Copies

1 On both the backup host and the primary host:

  a Shutdown both databases. For the cloned database on the backup host, you should perform log switches to make sure all online redo logs are switched to archive log files and that they are physically on the disk before you shutdown the cloned database. Or you can FTP over all online redo log files to the primary host, which can be used when performing database recovery.

  b Manually unmount all file systems used by both databases. Do not use the `vcdba_umount` utility in this step, which not only unmounts the file systems, but also removes the read-write virtual copy from the InServ Storage Server. If ASM is being used, unmount all involved ASM disk groups.

  c Deport the VxVM disk groups (used by datafiles and archive log destination).

  Example:

  On the backup host:

```
vxdg deport orcl920dg_042903142921
vxdg deport arch920dg_042903142921
```

  On the primary host:

```
vxdg deport orcl920dg
vxdg deport arch920dg
```

  Disk groups with trailing timestamps are created by Recovery Manager when performing a database backup. They can be found in the virtual copy repository.

2 On the InServ Storage Server, remove the VLUNs used by datafiles and archive log destination by issuing the `removevlun <vvname> <lun> <host>` command.

NOTE: If all VLUNs used by the database are removed, remember to recreate all of them after the rollback. Rollback only overrides virtual volumes used by datafiles and/or archive log destination (depending on which backup option the user performed for the specific timestamp).

3 Perform rollback on the backup host by executing the Recovery Manager `vcdba_rollback -s <oracle_sid> -p <primary_host> -t <timestamp> -v –w` command to roll back the read-write copy which is based on point-in-time, read-only snapshot when performing a database backup.

Example:

```
vcdba_rollback -s TEST920 -p pilot -t 042903142921 -v -w
```

4 On the InServ Storage Server, recreate all of the VLUNs, which were removed earlier. Us the same VLUN information by issuing the `createvlun <vvname> <lun> <host>` command.

5 On the primary host, run the `vxdctl enable` command and import the disk groups with the original names, and start all VM volumes. Wait until all disks are online.

Example:

```
vxdg -fC -n orcl920dg import orcl920dg_042903142921
vxdg -fC -n arch920dg import arch920dg_042903142921
vxvol -g orcl920dg startall
vxvol -g arch920dg startall
```

d Run the `vxdisk list` command to see if all volume disks are online and belong to the original names.

Example:

```
pilot:# vxdisk list
DEVICE       TYPE      DISK         GROUP        STATUS
c0t0d0s2     sliced    -            -            error
c2t0d0s2     sliced    disk01       rootdg       online
c2t0d41s2    sliced    orcl92001    orcl920dg    online
c2t0d42s2    sliced    orcl92002    orcl920dg    online
c2t0d43s2    sliced    orcl92003    orcl920dg    online
c2t0d44s2    sliced    orcl92004    orcl920dg    online
c2t0d45s2    sliced    orcl92005    orcl920dg    online
c2t0d46s2    sliced    orcl92006    orcl920dg    online
c2t0d47s2    sliced    orcl92007    orcl920dg    online
c2t0d48s2    sliced    arch92001    arch920dg    online
c2t0d49s2    sliced    arch92002    arch920dg    online
```

e Run the `fsck` command and mount all the file systems. If ASM is being used, mount all involved ASM disk groups.

f Recover the database using the new control file generated from the `vcdba_rollback` command. The name of the file is `ascii_controlfile_for_rollback`, and it is located in the virtual copy repository on the backup host. It also shows on the backup host screen when the rollback is done. Copy the ascii control file from the backup host to the primary host.

6 (Optional) Recover the cloned database on the backup host as follows:

NOTE: After performing the rollback, if you still want the cloned database on the backup host up and running, the following steps should be performed. Otherwise, this section can be skipped.

a On the InServ Storage Server, recreate all VLUNs previously removed by issuing the `createvlun <vvname> <lun> <host>` command.

b On the backup host, run the `vxdctl enable` command and import the disk groups using the same name as when you deported them.

Example:

```
vxdg import orcl920dg_042903142921
vxdg import arch920dg_042903142921
```

c On the backup host, run the `vxdisk list` command to make sure all volume disks are online and belong to the correct disk groups.

d On the backup host, mount all file systems previously used by the cloned database.

e On the backup host, start up the database.

8.3.2 Rollback with Read-Only Virtual Copies

To rollback read-only virtual copies, perform the following:

1. On the primary host, perform step 1 and step 2 on page 8.2. The only exception is that no action is needed on the backup host at this time.
2. On the backup host, execute the Recovery Manager `vcdba_rollback -s <oracle_sid> -p <primary_host> -t <timestamp> -v` command to roll back the specified read-only virtual copy.

   Example:

```
vcdba_rollback -s TEST920 -p pilot -t 042903142921 -v
```

3. Recover the database on the primary host. See step 4 and step 5 on page 8.5. When performing the import, no disk group names need to be changed.

9
Using Remote Copy with Recovery Manager

In this chapter

9.1 Overview

3PAR Recovery Manager provides three methods to utilize 3PAR Remote Copy for periodic synchronization:

- Graphic User Interface (GUI)
- Menu-driven application
- Command Line Interface (CLI)

Each method of Remote Copy is implemented by calling the following utility: `/opt/3par/vcdbaora/bin/vcdba_rsync`

The following figure illustrates the relationship between the primary and the backup hosts, and the primary/local and secondary/remote InServ Storage Servers:

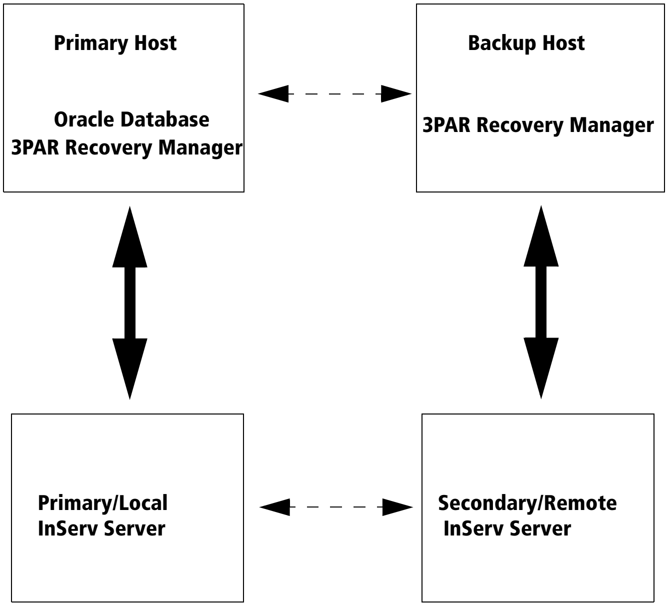


Figure 9-1. Remote Copy and Recovery Manager Relationship

The `vcdba_rsync` command uses the CLI command `syncrcopy` to periodically push the changed data from the primary/local InServ Storage Server to the secondary/remote InServ Storage Server. The time required for this process depends on the data volume changed in the primary database from the last synchronization, I/O load on both InServ Storage Servers, and the network speed.

Each time `vcdba_rsync` is executed, with either the `online` or `offline` option, Recovery Manager synchronizes the volumes on the secondary/remote InServ Storage Server with changes from the database on the primary/local InServ Storage Server. After the synchronization process is finished, Recovery Manager creates virtual copies for volumes on the secondary/remote InServ Storage Server. Those virtual copies constitute a consistent point-in-time backup image for the primary database. The primary database related files and information, such as `init.ora`, the Oracle password file, the binary control file (compressed format), the ASCII control file, datafile information, and tablespace information are saved in a virtual copy repository on a backup host. A virtual copy repository directory is created as `/etc/3par/solutions/<primary_host>.ora.<oracle_sid>/<timestamp>`

For example:

```
/etc/3par/solutions/right.ora.ISS920/032103170642
```

Virtual copies exist on the secondary/remote InServ Storage Server where they can later be mounted and used to clone the primary database. In addition, the virtual copies can also be backed up to a tape library or other inexpensive storage devices to keep a consistent point-in-time image of the primary database.

9.2 System Configuration

> **NOTE:** Before using this utility, ensure that all 3PAR Recovery Manager requirements are met, the Remote Copy licenses are installed on both the primary/local InServ Storage Server and the secondary/remote InServ Storage Server and Remote Copy is properly configured on both InServ Storage Servers.

9.2.1 Recovery Manager's Remote Copy Requirements

Before using the Recovery Manager Remote Copy utility, the following must be set up:

- Primary/local and secondary/remote InServ Storage Servers must be correctly configured.
- Links among nodes within two InServ Storage Servers must be set up and targets related to the two InServ Storage Servers must be created.

- Either one or two Remote Copy group(s) must be created, which contain all virtual volumes used by datafiles and archive log destinations. The one group option requires that datafiles and archive log destinations are in the same group. The two group option rqeuires that the archive log destination(s) is in a different group from datafiles.
- Recovery Manager only supports the `mirror_config` policy (default) for the involved Remote Copy target.
- Recovery Manager only supports periodic synchronization and requires the period value set to zero for the involved Remote Copy group.
- If volume manager is being used, all volumes that are in the same disk group as the datafiles or archive log destinations must be admitted to the Remote Copy group.
- If ASM is being used, all volumes that are in the same ASM disk group as the datafiles or archive log destinations must be admitted to the Remote Copy group.
- Remote copy group must be started and in synchronized status.
- Refer to the *3PAR Remote Copy User’s Guide* to set Remote Copy targets, links, and groups.

After the above has been set up, a Recovery Manager configuration file must be created. There are three ways to create a configuration file.

On the backup host:

- Run `/opt/3par/vcdbaora/bin/vcdbagui` to start the Recovery Manager Graphical User Interface (GUI).

  or

- Run `/opt/3par/vcdbaora/bin/vcdba_main` to start the Recovery Manager menu-driven utility.

  or

- Run `/opt/3par/vcdbaora/bin/vcdba_config` to start the Command Line Interface (CLI).

Refer to the *4.9 Recovery Manager Configuration Files* on page 4.27 to setup the configuration file for Remote Copy.

9.3 Verifying Remote Copy Settings

9.3.1 Verifying the Primary/Local Remote Copy Setting

To verify the primary/local Remote Copy setting:

1. Log in to the primary host as root user.
2. Connect to the primary/local InServ Storage Server from the primary host using either SSH or RSH:

```
<primary_host># ssh <username>@<ss_name>
```

where:

- `<username>` is the InServ Storage Server user.
- `<ss_name>` is the system name of the primary/local InServ Storage Server, which is attached to the primary host.
- You are not prompted for a password if set up correctly.

3. Verify the Remote Copy ports.

```
cli% showport -rcip
```

NOTE: Ensure the ports are in the `ready` state.

The following is sample output from the `showport -rcip` command:

```
N:S:P State HW Address IP Address Netmask Gateway MTU
0:5:1 ready 0002B3C03DF2 193.1.1.1 255.255.255.0 - 1500
1:5:1 ready 0002B3C03E94 194.1.1.1 255.255.255.0 - 1500
```

4. Verify the Remote Copy primary/local group (datafile group and archive log group).

```
cli% showrcopy groups <group name>
```

where:

- <group name> is the Remote Copy group name of the virtual volumes where the datafiles of the database reside.

> **NOTE:** Ensure the group is in the Start state and in Periodic mode.

5 Verify the Remote Copy targets.

```
cli% showrcopy targets <target_name>
```

where <target_name> is the name of the remote target that has been created using creatercopytarget.

> **NOTE:** Ensure the target status is Ready.

6 Verify the Remote Copy links.

```
cli% showrcopy links
```

> **NOTE:** Ensure the link status is Up.

9.3.2 Verifying the Secondary/Remote Copy Setting

To verify the secondary/remote Remote Copy setting:

1 Log in to the backup host as the root user.

2 Connect to the secondary/remote InServ Storage Server from the backup host using either SSH or RSH:

```
<backup_host># ssh <username>@<ss_name>
```

where:

- <username> is the InServ Storage Server CLI user.
- <ss_name> is the system name of the secondary/remote InServ Storage Server, which is attached to the backup host.
- You are note prompted for a password if set up correctly.

3 Verify the Remote Copy ports.

```
cli% showport -rcip
```

The following is sample output from the showport -rcip command:

```
N:S:P State HW Address IP Address Netmask Gateway MTU
0:5:1 ready 0002B3C03DF2 193.1.1.1 255.255.255.0 - 1500
1:5:1 ready 0002B3C03E94 194.1.1.1 255.255.255.0 - 1500
```

4 Verify the Remote Copy secondary/remote groups (datafile group and archive log group).

```
cli% showrcopy groups <group_name>
```

where:

- <group name> is the name of the Remote Copy group which contains all virtual volumes used by database datafiles.

NOTE: Ensure the group is in the Start state and in Periodic mode.

5 Verify the Remote Copy targets.

```
cli% showrcopy targets <target_name>
```

where <target name> is the name of the remote target that has been created using creatercopytarget.

NOTE: Ensure the target status is Ready.

6. Verify the Remote Copy links.

```
cli% showrcopy links
```

NOTE: Ensure the link status is Up.

9.3.2.1 Starting and Synchronizing Remote Copy Groups

Before using Recovery Manager with Remote Copy, groups in both the primary/local and secondary/remote InServ Storage Servers should be started and in a synchronized state. Starting and synchronizing the groups can be achieved by executing the following CLI commands from the primary/local InServ Storage Server:

- startrcopygroup <group_name>

  where <group_name> is the name of the Remote Copy group which contains all virtual volumes used by database datafiles and archive log destinations.

NOTE: The CLI command showrcopy can be used to check the synchronization status.

Prior to Recovery Manager release 3.0.0, two Remote Copy groups were required if archive log mode was enabled; one for datafiles and one for archive log destinations. If you wish to use one group configuration (recommended), where all datafiles and archive log destinations are within the same Remote Copy group, be sure to synchronize the Remote Copy group after you reorganize your Remote Copy group members. You can do this by issuing the syncrcopy <group_name> command.

Failure to issue the `syncropy <group_name>` command can result in the subsequently issued `vcdba_rsync` command failing with the following errors:

```
Eagle IPC transport error: EA_PROCESS_DOWN     -- Message canceled because
of process down

3PAR1170: ERROR: Could not perform syncrcopy for specified virtual copy.
Could not find request handler: EAIPC_NOPHANDLE     -- No phandle is
available or found
```

9.4 Using Remote Copy

3PAR Remote Copy can be used to backup the primary database and clone the primary database.

Cloned databases can be used for testing, generating reports, or development purpose. The primary database can be cloned from the backup host or any other alternate backup host, which connects to the secondary/remote InServ Storage Server.

Recovery Manager provides the utility to mount the virtual copies and further clone the primary databases on the backup host.

Index

Revision History

Release level	Revision summary
320-200190 Rev A November 2009	First release of this manual to support product release 3.0.2.